

## **SIGNATURE SHEET**

The Global Command and Control System (GCCS) Joint Integrated Logistics Support Plan is:

SUBMITTED BY:

---

DEBRA BENTLEY  
Integrated Logistics Support Manager  
Global Command & Control System

---

ELLIS K. CONOLEY  
Colonel, USAF  
Program Manager  
Global Command & Control System

APPROVED BY:

---

JOHN GAUSS  
Rear Admiral, USN  
Deputy Director  
Joint Interoperability and Engineering Organization  
Defense Information Systems Agency

## SIGNATURE SHEET


The Global Command and Control System (GCCS) Joint Integrated Logistics Support Plan is:

SUBMITTED BY:

  
DEBRA BENTLEY  
Integrated Logistics Support Manager  
Global Command & Control System

  
ELLIS K. CONOLEY  
Colonel, USAF  
Program Manager  
Global Command & Control System

APPROVED BY:

  
JOHN GAUSS  
Rear Admiral, USN  
Deputy Director  
Joint Interoperability and Engineering Organization  
Defense Information Systems Agency

## CONCURRENCE SHEET

The following concur with the Global Command and Control System Joint Integrated Logistics Support Plan:

---

Richard Burgess  
Lieutenant Colonel, USAF  
Program Manager  
Air Force Global Command and  
Control System

---

Barry E. Wright  
Colonel, USA  
Project Manager  
Strategic and Theater Command &  
Control Systems

---


J. E. Vesely  
Colonel, USMC  
Program Manager  
Command Information System  
Marine Corps Systems Command

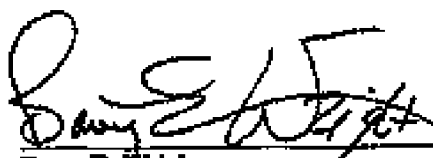
---


O. V. Combs  
Rear Admiral (Sel), USN  
C<sup>4</sup>I Systems Directorate  
SPAWAR (PD-70)


## CONCURRENCE SHEET

The following concur with the Global Command and Control System Joint Integrated Logistics Support Plan:

  
Richard Burgess  
Lieutenant Colonel, USAF  
Program Manager  
Air Force Global Command and  
Control System

  
Barry E. Wright  
Colonel, USA  
Project Manager  
Strategic and Theater Command &  
Control Systems

  
J. E. Vesely  
Colonel, USMC  
Program Manager  
Command Information System  
Marine Corps Systems Command

  
Matthew J. Rogers  
Captain, USN  
Program Manager  
Navy Command and Control  
Systems

## TABLE OF CONTENTS

PART I .....	1
1. INTRODUCTION .....	1
1.1 <u>Purpose</u> .....	1
1.2 <u>Background</u> .....	1
1.3 <u>Program Scope and Priority</u> .....	1
1.4 <u>Application</u> .....	2
1.5 <u>Iteration</u> .....	2
1.6 <u>Abbreviations and Acronyms</u> .....	2
2. SYSTEM DESCRIPTION .....	3
2.1 <u>Global Command and Control</u> .....	3
2.2 <u>Global Command and Control System</u> .....	3
2.3 <u>GCCS Infrastructure</u> .....	4
2.3.1 <u>Software Architecture</u> .....	4
2.3.2 <u>Hardware Architecture</u> .....	5
2.3.2.1 <u>Data Server</u> .....	5
2.3.2.2 <u>Application Servers</u> .....	5
2.3.2.3 <u>OPS/INTEL Server</u> .....	5
2.3.2.4 <u>Map Server</u> .....	5
2.3.2.5 <u>Automated Message Handling System (AMHS)</u> .....	6
2.3.2.6 <u>GCCS Premise Router</u> .....	7
2.3.2.8 <u>STU-III Devices</u> .....	7
2.3.2.9 <u>Multiplexers and Cryptographic Equipment</u> .....	7
2.3.2.10 <u>Fiber Duplexed Distribution Interface (FDDI)</u> .....	8
2.3.2.11 <u>Intelligent Hubs</u> .....	8
2.3.2.12 <u>Bridges/Routers</u> .....	8
2.3.2.13 <u>Clients</u> .....	8
2.3.3 <u>Perspective View</u> .....	9
2.3.3.1 <u>Organizational Perspective</u> .....	9
2.3.3.2 <u>Technical Perspective</u> .....	10
2.4 <u>Best-of-Breed Selection Process</u> .....	10
3. MANAGEMENT .....	10
3.1 <u>GCC Management Structure</u> .....	11
3.1.1 <u>Office of Primary Responsibility (OPR)</u> .....	11
3.1.1.1 <u>GCC General/Flag Officers Advisory Board</u> .....	12
3.1.1.2 <u>GCC Review Board</u> .....	12

3.1.1.3	<u>Functional Area and System Integration Working Groups.</u>	12
3.1.2	<u>Combat and Functional Unified Commands.</u>	13
3.1.3	<u>Military Services.</u>	13
3.2	<u>GCCS Management Structure</u>	14
3.2.1	<u>DISA Program Management</u>	14
3.2.1.1	<u>Deputy Director for C<sup>4</sup> and Intelligence Programs.</u>	14
3.2.1.2	<u>Joint Interoperability and Engineering Organization.</u>	14
3.2.1.3	<u>GCCS Migration Director.</u>	14
3.2.1.4	<u>DISA GCCS Task Force Organization.</u>	15
3.2.2	<u>Service Program Management.</u>	15
3.2.2.1	<u>Air Force.</u>	15
3.2.2.2	<u>Army.</u>	15
3.2.2.3	<u>Navy.</u>	15
3.2.2.4	<u>Marine Corps.</u>	15
3.3	<u>GCCS Integrated Logistics Support Management.</u>	15
3.3.1	<u>Air Force.</u>	15
3.3.2	<u>Army.</u>	15
3.3.3	<u>Navy.</u>	16
3.3.4	<u>Marine Corps.</u>	16
3.3.5	<u>GCCS Joint Integrated Logistics Support Management Team.</u>	16
3.3.5.1	<u>Air Force.</u>	16
3.3.5.2	<u>Army.</u>	16
3.3.5.3	<u>Marine Corps.</u>	16
3.3.5.4	<u>Navy.</u>	16
4.	<u>APPLICABLE DOCUMENTS</u>	16
PART II		17
1.	<u>PLANS, CONCEPTS, and STRATEGIES</u>	17
1.1	<u>Operational &amp; Organizational Plan</u>	17
1.1.1	<u>Global C<sup>4</sup>I Infrastructure</u>	17
1.2	<u>Operational Performance Requirements.</u>	17
1.2.1	<u>WAN Infrastructure</u>	18
1.2.2	<u>Network Management</u>	18
1.2.3	<u>Remote Users</u>	18
1.2.4	<u>Database Management</u>	18
1.2.5	<u>Joint Operation Planning and Execution System (JOPES)</u>	18
1.2.6	<u>Global Status of Resources and Training System (GSORTS)</u>	18
1.2.7	<u>Joint Deployable Intelligence Support System (JDISS)</u>	18
1.2.8	<u>Reliability, Maintainability and Availability Parameters.</u>	18
1.2.8.1	<u>Site Reliability.</u>	18

1.2.8.2	<u>Component Reliability.</u>	19
1.2.8.3	<u>Maintainability.</u>	19
1.2.8.4	<u>Availability.</u>	20
1.2.8.5	<u>GCCS Mission Operational Availability (GMOA) Measurement.</u>	21
1.2.8.5.1	<u>Background.</u>	21
1.2.8.5.2	<u>GCCS Mission Operational Availability (GMOA) Measurement.</u>	21
1.2.8.5.3	<u>Mathematical Definition of GMOA Measurement.</u>	23
1.3	<u>System Support Risks</u>	24
1.3.1	<u>Funding</u>	24
1.3.2	<u>Network Management</u>	24
1.3.3	<u>Training</u>	24
1.3.4	<u>Post Deployment Software Support</u>	24
1.3.5	<u>Hardware and Software Maintenance</u>	24
1.3.6	<u>Software Tailoring and Configuration</u>	24
2.	<u>MAINTENANCE CONCEPT</u>	25
2.1	<u>Air Force</u>	25
2.2	<u>Army</u>	25
2.3	<u>Navy</u>	25
2.4	<u>Marine Corps</u>	25
3.	<u>LOGISTICS SUPPORT ANALYSIS</u>	26
4.	<u>ACQUISITION STRATEGY</u>	26
4.1	<u>Life Cycle Cost (LCC) Reduction Actions</u>	26
5.	<u>TEST AND EVALUATION CONCEPT</u>	27
5.1	<u>Integrated Test Program Schedule.</u>	27
5.1.1	<u>Developmental Test and Evaluation.</u>	27
5.1.1.1	<u>Test Facilities.</u>	27
5.1.2	<u>Operational Evaluation.</u>	28
5.2	<u>Interoperability Certification.</u>	28
5.3	<u>Test and Evaluation Management Responsibilities.</u>	28
5.3.1	<u>Army.</u>	30
6.	<u>ILS ELEMENTS</u>	30
6.1	<u>Maintenance Planning</u>	31
6.1.1	<u>Customer Management System/Hotline</u>	31
6.1.2	<u>Interim Hardware Maintenance Concept.</u>	31
6.1.2.1	<u>Sun Hardware and Solaris Operating System Software</u>	

Maintenance	32
6.1.2.2 CONUS Maintenance Support	32
6.1.2.3 OCONUS Maintenance Support.	33
6.1.2.4 FDDI Hub and Lan Concentrator Maintenance.	33
6.1.2.5 Top Secret Support System (TS3) Hardware Maintenance.	34
6.1.2.5.1 Network Encryption System (NES).	34
6.1.2.5.2 CS2600 Server	34
6.1.2.5.3 Unitec UT-200.	34
6.1.2.5.4 STU 1910 SAC.	35
6.1.2.6 SAT Maintenance.	35
6.1.2.7 Premise Router Maintenance.	35
6.1.3 Long Term Hardware Maintenance Concept	35
6.1.4 Software Maintenance	36
6.1.4.1 Software Problem Reports and Engineering Changes	36
6.1.4.1.1 Army.	36
6.1.4.1.2 Marine Corps	36
6.1.4.2 Commercial Software Products	37
6.1.4.3 Software Licenses	37
6.1.4.4 Software Maintenance Funding	37
6.1.5 Warranties	37
6.2 Personnel	37
6.2.1 Site Manpower Requirements	37
6.2.1.1 GCCS Site Coordinator (GSC).	38
6.2.1.2 GCCS Network Administrator (GNA).	38
6.2.1.3 GCCS System Administrator (GSA).	38
6.2.1.4 GCCS Database Administrator (GDBA).	39
6.2.1.5 GCCS Site Designated Approving Authority (GCCS Site DAA)	39
6.2.1.6 Site GCCS Security Officer (SGSO)	39
6.2.1.7 GCCS System Support Programmer (GSSP)	39
6.2.2 Service Personnel Requirements	40
6.2.2.1 Air Force	40
6.2.2.2 Army - Manpower and Personnel Integration (MANPRINT)	40
6.2.2.3 Navy	41
6.2.2.4 Marine Corps	41
6.3 Supply Support	41
6.3.1 Provisioning	41
6.4 Support Equipment	41
6.5 Technical Data	41
6.5.1 User's Manuals	43
6.5.2 Maintenance Manuals	43
6.5.3 Operations Manuals	44



6.5.4	<u>DISA/JIEO Configuration Management Department Library</u>	44
6.5.5	<u>Publication Updates</u>	44
6.5.6	<u>Reprocurement Data Package</u>	44
6.5.7	<u>Classified Data</u>	44
6.6	<u>Training</u>	44
6.6.1	<u>GCCS Training Master Plan</u>	45
6.6.2	<u>AETC Training Plan</u>	45
6.6.3	<u>JOPEs Training Organization Course Catalog</u>	45
6.6.4	<u>Training Concept</u>	45
6.6.4.1	<u>Technical Training</u>	45
6.6.4.2	<u>Functional Training</u>	46
6.6.5	<u>Training Methods</u>	46
6.6.5.1	<u>Resident Training</u>	46
6.6.5.2	<u>Mobile Training Teams (MTTs)</u>	46
6.6.5.3	<u>Interactive Courseware (ICW)</u>	46
6.6.6	<u>Courses of Instruction</u>	46
6.6.6.1	<u>Funding for Training</u>	47
6.6.7	<u>Sustainment Joint Training Strategy</u>	47
6.6.7.1	<u>Army AGCCS Training Site (ATS)</u>	47
6.7	<u>Facilities</u>	47
6.7.1	<u>Utility Requirements</u>	48
6.8	<u>Packaging, Handling, Storage and Transportation</u>	48
6.8.1	<u>Storage Modes</u>	48
6.8.2	<u>Transportation and Transportability</u>	48
6.8.2.1	<u>Shipping Requirements</u>	48
6.9	<u>Design Interface</u>	48
6.9.1	<u>Reliability, Availability, and Maintainability (RAM)</u>	48
6.9.2	<u>Standardization</u>	49
6.9.3	<u>Commonality</u>	49
6.9.4	<u>Interoperability</u>	49
6.9.5	<u>Security</u>	50
6.9.6	<u>Links</u>	50
6.9.7	<u>Availability</u>	50
6.9.8	<u>Information Priority</u>	50
6.9.9	<u>Flexibility</u>	50
6.9.10	<u>Compatibility</u>	50
PART III -	<u>MILESTONE SCHEDULE</u>	51
PART III		49
III.	<u>MILESTONE SCHEDULE</u>	49

PART IV .....	50
IV. FIGURES, TABLES and ANNEXES .....	50
1. FIGURES	
Figure 1 - GCCS Three-tier Client-Server Structure .....	5
Figure 2 - GCCS Site Hardware General Configuration .....	6
Figure 3 - DII Component Interrelationship .....	10
2. TABLES	
Table 1 -GCCS Version 2.1 Documentation .....	37
3. ANNEXES	
Annex A - Glossary of Abbreviations and Acronyms .....	A-1
Annex B - Applicable GCCS documents .....	B-1
Annex C - Distribution List .....	C-1

## PART I

### 1. INTRODUCTION

**1.1 Purpose.** The purpose of the Global Command and Control System (GCCS) Joint Integrated Logistics Support Plan (JILSP) is to provide, in one document, essential information for the successful accomplishment of the Integrated Logistics Support (ILS) Program for the GCCS. Although a part of the overall program management documentation, this plan is designed for use as a stand-alone document for ILS planning and action. This JILSP will serve primarily as a working document for those activities directly responsible for the planning, management, and execution of the ILS program or any portion thereof. It will also be used for information purposes by all major commands, subordinate commands, and defense agencies concerned with this acquisition. The following objectives are established for this JILSP:

- Identify and document logistics requirements and constraints
- Describe required logistics actions, tasks and milestones
- Ensure all relevant ILS elements have been considered
- Provide logistics information for milestone reviews and decisions
- Establish responsibilities for ILS program participants

**1.2 Background.** The Joint Staff developed Mission Need Statement (MNS) and Concept of Operations (CONOPS) provide the baseline for the functional requirement of GCCS. Assistant Secretary of Defense (ASD) for Command, Control, Communications, and Intelligence (C<sup>3</sup>I) and Chairman of the Joint Chiefs of Staff (CJCS) have provided the mandate for a single Command and Control (C<sup>2</sup>) system. The Military Communications Electronic Board (MCEB) defined the initial proof of concept definition for GCCS and the Joint Staff CJCS Instruction 6721.01 defines the process for nominating functions for integration into future versions of GCCS. Legacy Worldwide Military Command and Control System (WWMCCS) applications will be replaced by nominated systems from the Services and Agencies.

**1.3 Program Scope and Priority.** The GCCS will be a seamless, interoperable, open client/server system that is fully capable of supporting military operations in peacetime and throughout the broad spectrum of conflict up to nuclear war. It will consist of all necessary hardware, software, procedures, standards and interfaces for connectivity worldwide at all levels of command.

Future C<sup>2</sup> systems will be based on GCCS standards and interfaces and follow the Common Operating Environment (COE) defined by DISA as the Designated Development Agent (DDA) in concert with the Services and their representatives.

The GCCS program is the number one priority program in DISA and will provide peacetime and wartime C<sup>2</sup> capabilities that directly support a full spectrum of Joint and Service combatant operations. GCCS must be accorded a sufficiently high priority by the Services to ensure availability of financial and infrastructure resources to provide necessary support.

**1.4 Application.** This JILSP provides detailed management policies for life cycle logistics support of GCCS. The contents of this JILSP were developed in accordance with (IAW) Department of Defense (DoD) Instruction (DoDI) 5000.2, "Defense Acquisition Management Policies and Procedures;" and the joint requirements of Department of the Army Regulation (AR) 700-129/Chief of Naval Operations Instruction (OPNAVINST) 4105.2A/Air Force Supplement 1 to DoDI 5000.2 /Marine Corps Order (MCO) 4110.2, "Management and Execution of Integrated Logistic Support (ILS) for Multi-Service Acquisitions." This JILSP presents program management-level logistics information to be used in logistics planning during all phases of the GCCS life cycle.

This document may contain specific references to selected Services/Agencies within the subsections of the document, where applicable and appropriate details are available. Lack of specific comments pertaining to the Services/Agency in this version of the document does not indicate exclusion from the integrated logistics support planning process.

**1.5 Iteration.** This is the first iteration of the GCCS JILSP. Changes to this JILSP will be distributed based on program changes. Addressees are encouraged to submit recommended changes/updates to the ILS Manager at:

DISA/D23  
45335 Vintage Park Plaza  
Sterling, VA 20166-6701

**1.6 Abbreviations and Acronyms.** ANNEX A contains a glossary of acronyms and abbreviations used in this JILSP.

## 2. SYSTEM DESCRIPTION

This section provides an overview of the GCCS configuration, environment, and functional requirements. This JILSP condenses and presents the system description from key GCCS documentation referenced in Annex B.

**2.1 Global Command and Control.** Global Command and Control (GCC) encompasses the policies, procedures, trained personnel, and systems that support the Command and Control (C<sup>2</sup>) of forces, from the National Command Authorities (NCA), through the Joint Task Force and its Service components, during peace, crisis, and war. These policies, procedures, and systems include monitoring, planning, and executing mobilization, deployment, employment, sustainment, redeployment, and force regeneration activities associated with military operations.

**2.2 Global Command and Control System.** The GCCS is a comprehensive, worldwide network of systems which provide the NCA, Joint Staff, combatant and functional unified commands, Services, Defense agencies, Joint Task Forces and their Service components, and others with information processing and dissemination capabilities necessary to conduct C<sup>2</sup> of forces. GCCS is a means to implement the Command, Control, Communications, Computers, and Intelligence (C<sup>4</sup>I) for the Warrior concept. An evolutionary implementation strategy is being used to provide warfighters with their required operational capabilities. The GCCS "no grand design" philosophy lends itself to extensive user participation, incremental fielding, and shorter periods between update cycles.

The GCCS development approach employs an open, client-server environment under the COE definition. The Director for Command, Control, and Communications, and Computers (J-6) of the Joint Chiefs of Staff (JCS), serves as the GCCS Designated Approving Authority and appoints the GCCS Security Officer. The COE provides the standard environment for all future development of Service systems. The use of Commercial-off-the-Shelf (COTS) hardware and software is a primary consideration for the GCCS. The GCCS hardware and software must meet standards which support the GCCS COE, including DoD recommended data communications protocol standards described in Technical Architecture for Information Management (TAFIM), Volume 1 through 8, Adopted Information Technology Standards (AITS), and its related handbook, Information Technology Standards Guidance (ITSG).

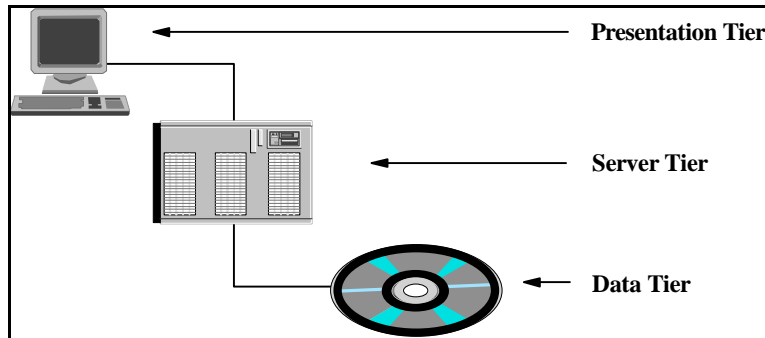
Client-server platforms and network equipment shall support Profiles for Open Systems Internetworking Technologies (POSIT) as described in Federal Information Processing Standards (FIPS) Publication 146-2. The GCCS is not being developed and fielded as a single configuration. GCCS is comprised of a variety of platforms. Specific configurations [e.g. Random Access Memory (RAM), Central Processing Units (CPUs), Disk Capacity, Printer type/model, Compact Disk Read Only Memory (CD ROM), Monitors, UPS, and Network Equipment] are driven by site specific requirements and will be described in individual Service and agency Facility Support Plans (FSPs), Material Fielding Plans (MFPs), and User's Logistics Support Summaries (ULSS).

GCCS is not a hardware acquisition project. It operates on a variety of platforms and is hardware independent to a certain extent. It will have a standardized COE and provide core applications to achieve warrior-specified performance requirements and interoperability objectives. The GCCS Program Office will evaluate and select for reuse applications from candidate systems recommended by the Services and Defense agencies, within the goals established for functional capabilities, performance, interoperability, and cost. The selection process is an objective, participatory evolution that will result in the integration of software applications certified by previous warfighters and endorsed by current warfighters.

**2.3 GCCS Infrastructure.** GCCS is a highly mobile, deployable C4I system that supports forces for joint and combined operations throughout the spectrum of conflict anytime and anywhere in the world with compatible, interoperable, and integrated C4I Systems. GCCS "communications" are provided by the Secret Internet Protocol Router Network (SIPRNET) Wide Area Network (WAN), by Services and Agencies (S/A) WANs, and by Commander in Chief (CINC) and S/As Local Area Networks (LANs). Additionally, many secondary communications paths are provided by the individual S/As in support of their remote GCCS users. Both the WANs/LANs and the secondary communications paths take advantage of relatively stable telecommunications industry standards. The GCCS "computers" are provided by cooperative research and development efforts among DISA, the S/As, and other DoD organizations. Again, these platforms take advantage of evolving standards in the information systems industry. Together, the communications and computers of the GCCS will make up a part of the Defense Information Infrastructure (DII). The following sections will clarify both the software and hardware approaches taken by the GCCS to perform the C2 mission. Emphasis will be placed on the communications and computer aspect.

**2.3.1 Software Architecture.** The GCCS is a distributed computing system. The software and data supporting command and control functions are distributed across heterogeneous and interoperable computers connected through the secret worldwide SIPRNET. This distributed computing is implemented through a three-tier client-server architecture: the presentation (user-interface), the server (functional), and the data storage tiers. The presentation tier includes mission-specific joint, service, and command unique applications in addition to standard and COTS user interface elements such as X-Windows or Motif. The server tier includes functions (server-resident applications for mission applications, office automation, systems management, etc.), and the components upon which these functions reside. The data storage tier, linked to existing systems and applications, includes data storage and database management systems.

The goal of this approach is to insulate the application logic from the presentation and data storage software. The three-tier architecture, shown in Figure 1, addresses the issues of integrating object, relational, and legacy systems migrating to client-server technology. The three tiers, although pictured as three separate components, represent a logical separation and may reside on one, two, or more different hardware platforms.



**Figure 1 - GCCS Three-tier Client-Server Structure**

**2.3.2 Hardware Architecture.** Each GCCS site has a core set of hardware and software. While some of the hardware directly correlates to the three-tiered client-server structure identified above other components are used to provide the GCCS communications infrastructure within each site. Figure 2 is representative of a primary GCCS site. The following paragraphs explain the functions of each hardware component within the GCCS suite of equipment.

**2.3.2.1 Data Server.** The data server represents the third tier, the data storage tier, in the software model. The typical data server is a SUN Sparc 1000 with at least 32 Gigabytes (GB) of mirrored storage from a RAID Array. Some of the GCCS sites have SUN Sparc 2000 instead of the Sparc 1000 for their data storage device. Variances in disk capacity and Rapid Access Memory (RAM) size will exist within the GCCS as a whole.

**2.3.2.2 Application Servers.** The next set of devices are the application servers. These are SUN Sparc 20s with most servers having 4 GBs of hard disc storage. They are the second tier, the server tier, in the software model. Initially, each site will have two application servers. Depending on the size and complexity of the site it is possible there will be more servers. The application servers are sized to support 5 concurrent XWindows sessions or 20 TELNET sessions. Individual differences in applications servers will cause these numbers to fluctuate.

**2.3.2.3 OPS/INTEL Server.** The next device is an OPS/INTEL server. A select few of the GCCS sites have been identified to receive an additional SUN Sparc 20 after IOC to serve in this capacity. The device has 4GBs of hard disc storage.

**2.3.2.4 Map Server.** Next is the MAP server. Some GCCS sites will have the need to store a large volume of maps at their location. Another SUN Sparc 20 is identified to be this server and will be fielded after IOC. The hard disk size and amount of RAM required in this device is still being determined.

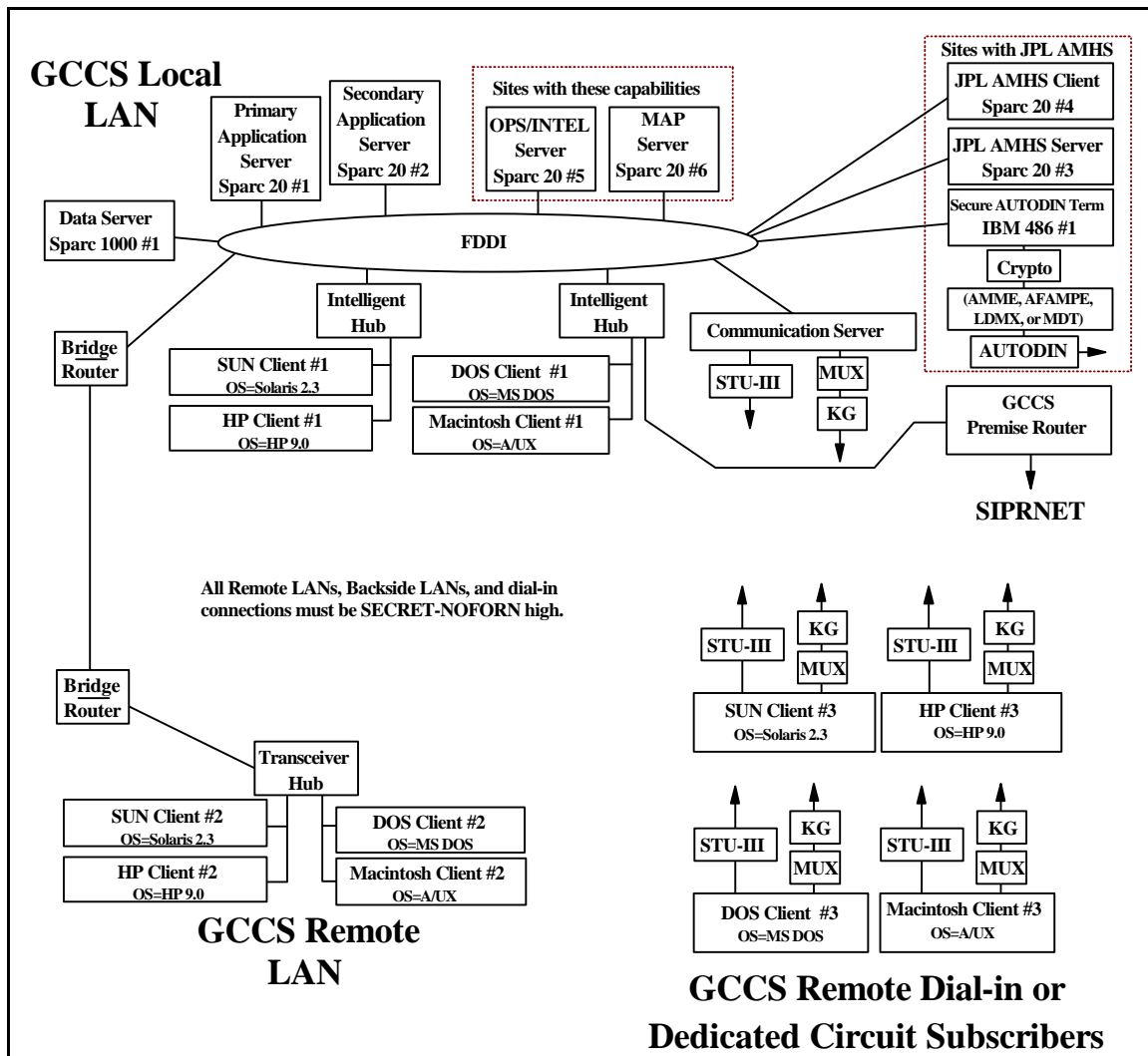


Figure 2 - GCCS Site Hardware General Configuration

**2.3.2.5 Automated Message Handling System (AMHS).** The GCCS AMHS is the Army system produced by the NASA Jet Propulsion Laboratory (JPL). In actuality, two configurations will exist for the AMHS suite of equipment based on the volume of message traffic processed at the GCCS site. Shown in Figure 2 is the high volume solution. It consists of two SUN Sparc 20s. One serves as the AMHS server while the other is the AMHS dedicated client. The dedicated Sparc 20 client workstation represents the one used by the operator responsible for the AMHS. It should be noted any of the GCCS workstations can be loaded with the AMHS client software. The difference between the high and low volume solutions is the low volume solution does not have the two dedicated Sparc 20s. Instead, separate file systems are reserved on the database server for the AMHS function. The next device in the AMHS suite is the Secure AUTODIN Terminal (SAT) which contains a specialized communications card for interfacing



with the AUTODIN message system. The SAT computer is an Intel 486 based computer operating with the Microsoft Disk Operating System (MS DOS). The next component in the AMHS suite is the cryptographic devices feeding data to the SAT. A large variety of cryptographic devices are used with each being site specific. The next device in the AMHS suite can be one of seven different components. These components (AMME, AFAMPE, LDMX, MDT, etc) are an integral part of the AUTODIN feed to ensure 100% message delivery. And finally, there is the 4800 bits per second (bps) AUTODIN circuit feed. There will be a wide variety of AMHS configuration. Each configuration will have to undergo certification testing. One stipulation of AMHS certification is that the GCCS LAN, all remote LANs, all backside LANs, all remote dial-in subscribers, and dedicated circuit subscribers must be protected at the Secret-NOFORN classification level otherwise certification will be denied at that particular GCCS site.

**2.3.2.6 GCCS Premise Router.** The GCCS Premise router is part of the GCCS site's LAN infrastructure. This represents the gateway point out to the SIPRNET WAN. The majority of GCCS premise routers in use are manufactured by Cisco. The premise routers were supplied to the IOC sites by DISA but they are owned and operated by the individual GCCS sites. As such, it is highly possible that the existing premise routers may be swapped out in the future by some GCCS sites to install a larger capacity router to accommodate their specific mission needs. This will be especially true where the GCCS site has a large campus environment (many buildings linked together by routers or bridges) to support. The replacement routers used by the sites will not have to be from the Cisco product line so long as they are compatible devices.

**2.3.2.7 Communications Server (CS).** The CS is part of the site's LAN infrastructure. The devices initially being provided by DISA but owned and operated by the GCCS sites are the CISCO 2511-CSs. These CSs have two serial ports, one ethernet port, and 16 asynchronous dial-in ports. The CSs will server two types of users. The first are users who dial into the GCCS site using a Secure Telephone Unit - III (STU-III) to gain access to the GCCS infrastructure. The second set of users are those who are connected to the GCCS site via low speed dedicated multiplexer circuits. Authentication and access control will be performed at the CS. The CS is considered an access point to the general DoD secret-level LAN/WAN infrastructure and must be protected as such.

**2.3.2.8 STU-III Devices.** The STU-III devices connected to the CSs must be new generation STU-IIIs to accommodate the bandwidth requirements of the GCCS applications. It is recommended the GCCS sites use models such as the AT&T Model 1910 STU-III. This particular device has a 14.4 kbps modem engine and obtains throughput speeds of 38.4 kbps using internally supplied compression algorithms. Built in error correction algorithms should also be activated to overcome poor quality telephone lines. It is the responsibility of the GCCS site to provide STU-IIIs and telephone lines to support their dial-in requirements.

**2.3.2.9 Multiplexers and Cryptographic Equipment.** The next set of devices would be the

multiplexers and cryptographic equipment used to support the dedicated circuit remote subscribers. This group of users are carryovers from the slow speed dedicated connections that existed within the WWMCCS community. A majority of these connections are 2.4 and 4.8 Kilo-Bytes per second (kbps) in the WWMCCS environment. The vast majority of GCCS applications will not run over this slow of speed circuit. A minimum speed of 28.8 kbps is recommended for the GCCS environment. It may be cost effective for remote GCCS users to migrate from dedicated multiplexer circuits over to a dial-in basis using STU-III technology provided their mission needs can still be met.

**2.3.2.10 Fiber Duplexed Distribution Interface (FDDI).** The FDDI is a high speed LAN technology used to interconnect all of the major components of the GCCS site. This includes the data server, the application server, and the intelligent hubs. In some cases the premise router may also be connected to the FDDI ring instead of what is shown in Figure 2. DISA is providing the FDDI equipment to the primary GCCS sites.

**2.3.2.11 Intelligent Hubs.** The intelligent hubs are the next devices. These are LAN infrastructure devices that allow the FDDI LAN to be connected to the site's normal ethernet LANs. The intelligent hubs provide the translation function of the LAN speeds and protocols. It's important to note that individual LAN infrastructures will vary greatly from site to site. DISA provided intelligent hubs during the initial equipment deployment.

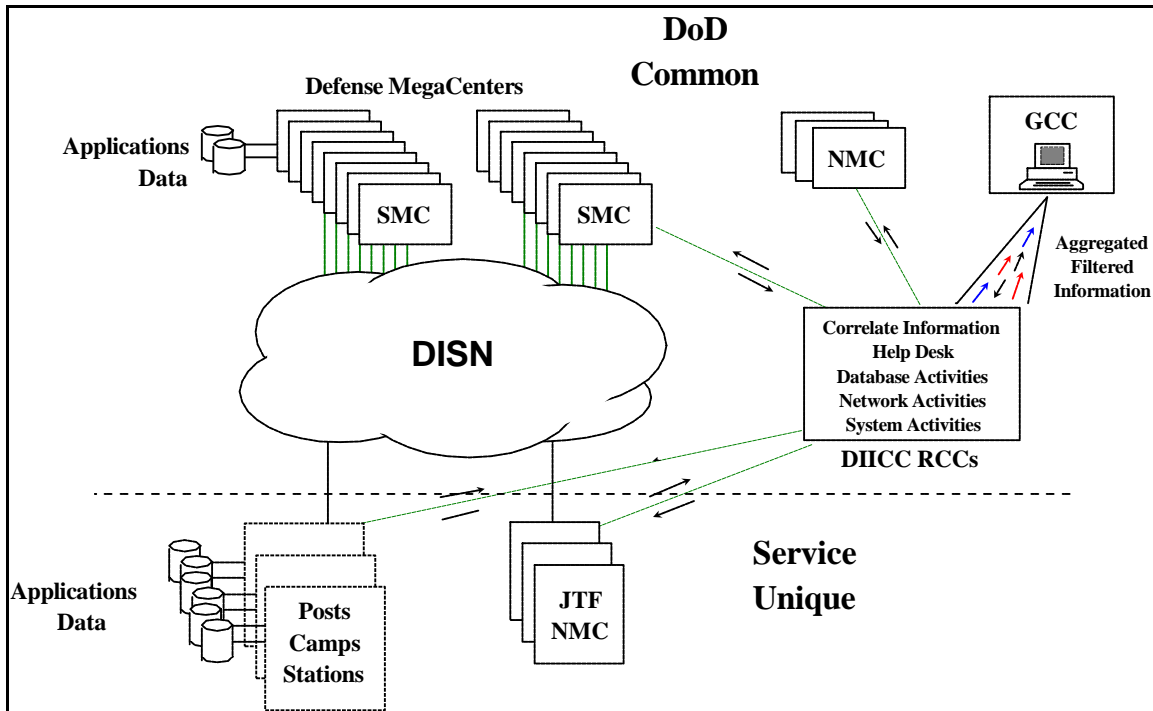
**2.3.2.12 Bridges/Routers.** Bridges/Routers will be very particular to each GCCS site. In most cases a GCCS site will not exist within a single building or facility nor contain a single LAN segment. It is highly likely there will be multiple buildings within a close geographical area to form a campus environment. This campus environment would consist of a group of individual LANs interconnected by additional routers or bridges to form the GCCS site. The additional routers or bridges are not limited to interconnecting those sites within close geographical proximity. They could also be used to tie in GCCS Remote LANs that are large distances away. The existence of these campus environments and GCCS Remote LANs is one of the primary driving factors for performing network management within the GCCS environment.

**2.3.2.13 Clients.** The final group of devices are the clients, the actual users of the GCCS software. The users represent the presentation tier of the three-tier software model. The hardware platforms used by the clients can vary greatly. The GCCS places a strong emphasis on software and not on a hardware dependency. The GCCS software is being developed to operate on the SUN Solaris 2.3 or the Hewlett Packard (HP) HP-UX-9.0.1 operating systems. To operate the GCCS software suite, the hardware platform must support the SUN Solaris 2.3 or the Hewlett Packard (HP) HP-UX-9.0.1 operating systems. A hardware platform that uses a different operating system can still be used as a GCCS client. This client would only have to run a standard XTerminal/XWindows application software package to reach a GCCS application server. It would then have all the functionality of a SUN or HP based client. Clients identified so far on the GCCS are SUN Sparc 5s, SUN Sparc 10s, SUN Sparc 20s, TAC-3s, future TAC-4s, Macintosh

Ilfxs (also referred to as HoneyMacs or WIS workstations), and a variety of MS DOS based platforms. The hard disk and RAM requirements of each platform depends on what the user wants to operate on that particular hardware platform. If they function strictly as an XTerminal devices then the hardware requirements are not as great as a workstation that wants to run GCCS applications resident in the platform. Another import point worth noting is that a few of the GCCS applications exist in Macintosh Ilfxs or MS-DOS operating system. The hardware requirements of GCCS client workstations are left to the discretion of the GCCS sites based on their mission needs.

**2.3.3 Perspective View.** The GCCS architecture may be viewed from organizational and technical perspectives. The organizational perspective focuses on the user. The technical perspective focuses upon the three-tier client-server software structure, hardware, and LAN/WAN technologies used within the GCCS. The genesis of these perspectives is in the interpretation of DoD policy and mission statements and the nature of existing and planned technical initiatives. For example, policy and mission require cooperation among assigned forces in a Combined/Joint Task Force (C/JTF), thus leading to the organizational perspective. The GCCS sites derive their physical relationship by the interconnection provided by the Defense Information System Network (DISN) SIPRNET WAN, leading to the technical perspective. Both perspectives are explained in greater detail below.

**2.3.3.1 Organizational Perspective.** The organizations using the GCCS are the NCA, CINCs, Components, C/JTF, and assigned Forces. Additionally, DII components that could support the GCCS in the future are the Defense Mega-Centers (DMCs), the Integrated Management Centers (IMCs), base-level communications and the DISN. A complex logical relationship will exist among the GCCS community as well as between those external organizations and information sources such as national assets from weather and emergency relief agencies and international military agencies like the North Atlantic Treaty Organization (NATO). Effective support of this relationship depends upon extensive technical support from DII components which among themselves comprise an extensive inter-component relationship. An example of this complex relationship within the DII can be seen by referring to Figure 3. The DMCs may contain "reachback" information repositories at the secret classification level that a GCCS user needs to access. The information repositories are maintained by the DISA System Management Center (SMC) responding to the direction of a DISN Regional Control Center (RCC) operated by DISA. A user at one GCCS site located on a campus, post, or base may wish to correlate reachback information from their location with reachback information at one of the Mega-Centers. The information repositories at the Mega-Centers are maintained by the DISA DISN portion of the DII and are outside the normal boundaries of the GCCS Management Center (GMC) for the GCCS. Should anomalies occur during the user's correlation process, the GCCS site may need to rely upon their GCCS System Administrator to consult with a peer administrator at the SMC. The following figure helps to show the DII interrelationship.



**Figure 3 - DII Component Interrelationship**

**2.3.3.2 Technical Perspective.** The three-tier client-server structure is the starting point of the GCCS architecture's technical perspective. This structure coupled with the hardware and LAN/WAN technology used gives a clear technical picture of the GCCS. The technical perspective may be applied to the organizational perspective above to show how different organizations will physically interconnect. The GCCS sites each operate their own LANs, an example of which is shown in Figure 2 previously. These LANs are interconnected by the SIPRNET WAN of DISN.

**2.4 Best-of-Breed Selection Process.** The selection process chooses, from among all candidate systems or applications, the best system or application suited for a specific function to support the warfighter and then migrates those capabilities into GCCS. The CINCs have identified the core functions as Crisis Planning, Force Deployment, Force Employment, Force Status, Logistics, Air Operations, Fire Support, Intelligence, Personnel, Position, and Narrative Information. The new systems need to be interoperable by being menu/mouse driven, be available for user training at their home station, and provide user-friendly displays with graphics.

### 3. MANAGEMENT

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6721.01, "Global Command and Control Management Structure" establishes the responsibilities of the Joint Staff, Services,

Defense agencies, combatant and functional unified commands, and other activities regarding management of GCC, and a management structure with assigned responsibilities for GCC.

**3.1 GCC Management Structure.** CJCS is responsible for policy guidance and oversight of GCC. This guidance is transmitted to the Director, Joint Staff, and the Director for Operations (J-3 in particular) for implementation. The GCC Management structure is designed to provide the following.

- Oversight of the C<sup>2</sup> requirements for the NCA, Joint Staff, Service headquarters, combatants and functional unified commands.
- Review, validate, approve, and prioritize requirements and select the best candidates for integration into the system.
- Approve policies and procedures that support joint C<sup>2</sup> requirements.
- Govern selection of applications and improvements for integration into GCCS. This includes the approval and selection of Automated Data Processing (ADP) systems for migration and integration into GCCS to satisfy joint command and control requirements.
- Manage the GCCS implementation and coordinate policy and development functions for GCCS.

**3.1.1 Office of Primary Responsibility (OPR).** The Director for Operations, J-3, Joint Staff has been assigned as the OPR and is responsible for the development of the GCC CONOPS, policy and functional requirements. In addition, the following duties are assigned J-3 as the OPR:

- Approves the GCCS Planning, Programming and Budgeting System (PPBS) for funds managed by the Joint Staff and DISA. Reviews and makes recommendations to Services' GCCS spending plans and PPBS submissions that support Joint and Service GCCS requirements.
- Approves the development and implementation plans for the processes and capabilities that support GCC.
- Approves GCC policy.

- Ensures the GCC development strategy is consistent with the current planning and execution procedures for the national strategy and the Unified Command Plan (UCP).
- Serves as chairperson of the GCC Flag/General Officer Advisory Board.

The OPR is supported by a general/flag officers advisory board, a review board, and working groups.

**3.1.1.1 GCC General/Flag Officers Advisory Board.** This J-3 chaired board consists of flag officers or their flag level representatives from all Joint Staff directorates, Services, combatant and functional unified commands, and DISA. The responsibilities of this board include the following:

- Advising the OPR on the priority and execution of GCC requirements, policy and development and implementation plans.
- Providing the CJCS, Services, combatant and functional unified commands, and the Joint Staff with information concerning GCC requirements, objectives, and milestones.
- Ensuring that Service Coordination is accomplished on those actions affecting budget and resources.
- Identifying, discussing and taking action on any unresolved GCC issues and or recommendations forwarded by the GCC Review Board or presented by a member of the General/Flag Officers Advisory Board.
- Approving new functionality for development and/or migration into GCCS.

**3.1.1.2 GCC Review Board.** The Vice Director for Command, Control, Communications and Computer Systems Directorate J-6 chairs the GCC Review Board which reviews GCC requirements and issues. It forwards those requiring action to the General/Flag Officers Advisory Board with recommendations. This board evaluates the technical, functional, training, and funding criteria in determining which applications will be forwarded and their overall implementation prioritization to the GCC General/Flag Officer Advisory Board. It, also, directs the execution of those validated requirements that support the OPR approved development and implementation plans. Members to this board consist of O-6 representatives from all Joint Staff directorates, Services, combatant and functional unified commands, and the chairs from the Functional Area and Systems Integration Working Groups.

**3.1.1.3 Functional Area and System Integration Working Groups.** Permanent Functional Area and Systems Integration Working Groups are assigned to nine areas that are routinely

involved with GCC. Ad hoc working groups are created as needed, to examine specific issues. Each group is chaired by a Joint Staff directorate which is responsible for ensuring that the group can accomplish its assigned and implied taskings. Working groups meet as frequently as required. At a minimum, each group will include representatives at the O-5 level or below from the Joint Staff directorates, services, combatant and functional unified commands and/or their component commands, and DoD agencies. Permanent working groups have been assigned to the following areas:

- GCC Intelligence Functional Area Working Group
- GCC Employment and Crisis Action Functional Area Working Group
- GCC Sustainment Functional Area Working Group
- GCC Deployment/Redeployment Functional Area Working Group
- GCC C4 Systems Integration Working Group
- GCC Deliberate Planning Working Group
- GCC Training Working Group
- GCC Readiness Working Group
- GCC Modeling and Simulation Working Group

**3.1.2 Combat and Functional Unified Commands.** Combat and functional unified commands are tasked with providing the following:

- Representatives to the three GCC Management Boards and attending other working groups as required.
- Providing emerging requirements to the appropriate working groups for actions and provide test beds for GCCS prototypes.
- Oversee, in coordination with the Services, the operation and maintenance of the GCCS sites.

**3.1.3 Military Services.** The Military Services are tasked with providing the following:

- Representatives to the three GCC Management Boards.
- Establishing GCCS functional and technical coordination points of contact.
- Program, plan and budget for Service responsible GCCS requirements.

- Operate and maintain GCCS sites in coordination with the combatant and functional unified commands and components.
- Providing the mechanism through which the Services are advised of GCCS activity which may impact Service resources and budgets.

**3.2 GCCS Management Structure.** The Defense Information Systems Agency (DISA) serves as the executive agent of the Joint Staff for GCCS and for the transition efforts that migrate current systems to GCCS. The long-haul communications networks that supports GCCS connectivity to each site's GCCS premise router is also included within this charter.

**3.2.1 DISA Program Management.** The DISA Program Manager provides oversight and direction of activities in DISA to:

- Integrate, test, and field all GCCS applications in accordance with Joint Staff guidance.
- Develop and maintain GCCS configuration management with direct user involvement IAW the GCCS configuration management policy.
- Provide program and other staff/flag briefings.
- Develop specific application software and appropriate functional and technical documentation for all GCCS applications.
- Develop funding and appropriate budgeting for GCCS.

**3.2.1.1 Deputy Director for C<sup>4</sup> and Intelligence Programs.** Deputy Director for C<sup>4</sup> and Intelligence (C<sup>4</sup>I) Programs (D2) manages and directs all information system acquisition programs such as GCCS that are assigned to DISA, and ensures the establishment and control of life cycle management support for those systems.

**3.2.1.2 Joint Interoperability and Engineering Organization.** The Joint Interoperability and Engineering Organization (JIEO), Director of the DISA field activity, conducts the implementation of GCCS.

**3.2.1.3 GCCS Migration Director.** The Migration Director/GCCS Program Management Office (D23) was chartered by the Director, DISA on 15 August 1993, to provide high level oversight, monitoring, guidance and coordination with Joint Staff on requirements and direction to activate GCCS sites, and ensure that stated Mission Needs (from the Joint Staff MNS) are met.



**3.2.1.4 DISA GCCS Task Force Organization.** The GCCS Task Force organization is comprised of the Program Manager (PM), service representatives, and eight functional managers. The functional managers represent the following areas:

- Program Controls
- Implementation
- Product Assurance
- Logistics
- Software Products
- System Center
- GCCS Engineering
- Data Base

**3.2.2 Service Program Management.** The following Program Management Offices have been established by the Services.

**3.2.2.1 Air Force.** The Air Force Program Office (ESC/AVN) is located at Hanscom Air Force Base (AFB), Boston, MA.

**3.2.2.2 Army.** The Strategic and Theater Command and Control System (STCCS) Program Management Office (PMO) is responsible for managing, planning and integrating AGCCS components into GCCS. STCCS provides technical support, software development, and Systems Engineering & Integration (SEI).

**3.2.2.3 Navy.** Space and Naval Warfare Systems Command (SPAWAR) C<sup>4</sup>I Systems Directorate PD70 is responsible for program management of Navy GCCS implementation.

**3.2.2.4 Marine Corps.** The United States Marine Corps (USMC) GCCS Project Office (PO) is located within the Marine Corps Systems Command (MARCORSYSCOM) C<sup>4</sup>I, Command Information Systems (CIS) at Quantico, Virginia.

**3.3 GCCS Integrated Logistics Support Management.** The GCCS Integrated Logistics Support Manager (ILSM), D42, is matrixed into the PMO by the Deputy Director, Logistics and Procurement, D42. The ILSM is responsible for the management and implementation of all elements of integrated logistics support for GCCS and the two DISA supported sites.

**3.3.1 Air Force.** The Deputy Program Manager for Logistics (ESC/AVL) is located at Hanscom Air Force Base, Boston, MA.

**3.3.2 Army.** The Logistics Division of the STCCS PMO provides policy and guidance to the AGCCS Project regarding Test & Evaluation (T&E), configuration management, training, maintenance, and Manpower and Personnel Integration (MANPRINT). The Logistics Division

reviews Joint ILS policy and guidance and incorporates into AGCCS ILS planning and implementation, ensures ILS goals and thresholds are integrated into project decisions, system software designs, and the acquisition process; coordinates ILS planning, requirements, and actions with DoD and Department of Army (DA) components; and participates in Joint, Inter-service, and AGCCS ILS reviews and meetings.

**3.3.3 Navy.** Space and Naval Warfare Systems Command (SPAWAR) Head JMCIS/C4I Common Products Logistics Division (PD 72L1) is the Navy's ILS Manager.

**3.3.4 Marine Corps.** Collocated with the Project Officer, is the Integrated Logistics Support Officer (ILSO) matrixed to the PO from Project Support Logistics (PSL). The ILSO works in the Assistant Program Manager Logistics (APML) cell at MARCORSYSCOM, C<sup>4</sup>I, CIS, Quantico, VA. The Marine Corps GCCS Project Officer and the ILSO support the DISA ILS manager on all programmatic and logistics matters related to the Marine Corps participation in the GCCS program. USMC configuration management will be controlled by Marine Corps Technical Software Support Activity (MCTSSA).

**3.3.5 GCCS Joint Integrated Logistics Support Management Team.** The DISA Joint Integrated Logistics Support Management Team (JILSMT) will be chaired by the GCCS ILS Manager, and will provide program direction and problem resolution for all programmatic decisions associated with the ILS program. JILSMT members include representatives from the CINCs, Services, DISA, and the Joint Staff.

**3.3.5.1 Air Force.** The Air Force ILS Management Team (ILSMT) will be chaired by the Air Force ILS manager. Air Force ILSMT members include representatives from the Major Commands (MAJCOMs), Agencies, and Direct Reporting Units.

**3.3.5.2 Army.** The Army's ILSMT representative will be the STCCS Logistics Division.

**3.3.5.3 Marine Corps.** The Marine Corps' representative on the JILSMT will be the Marine Corps Systems Command Assistant Program Manager for Logistics, Decision Support Systems, Code PSL.

**3.3.5.4 Navy.** The Navy's representative on JILSMT will be the SPAWAR Joint Maritime Command Information System ILS Division Head, Code PD 72L1.

**4. APPLICABLE DOCUMENTS.** See ANNEX B.

## **PART II**

### **1. PLANS, CONCEPTS, and STRATEGIES**

**1.1 Operational & Organizational Plan.** GCCS is the single joint command and control system. The GCCS Concept of Operations defines the roles, responsibilities, and relationships within GCCS Command and Control Infrastructure. GCCS includes both fixed and highly mobile, deployable platforms that support forces for joint and combined operations throughout the spectrum of conflict anytime and anywhere in the world with compatible, interoperable, and integrated C<sup>4</sup>I systems. GCCS incorporates the policies, procedures, reporting structures, trained personnel, automated information processing systems, and connectivity to provide information necessary to plan, deploy, sustain, and employ forces. It supports the range of operations along the military continuum as envisioned by national military strategy. It also allows a response to natural emergencies and/or man-made disasters when military support is appropriate.

**1.1.1 Global C<sup>4</sup>I Infrastructure.** A global C<sup>4</sup>I infrastructure is established to accommodate the widest possible range of missions and operational scenarios by allowing users to enter the infrastructure at anytime and anyplace in the execution of their mission. The system is supported by the DISN infrastructure that provides the forces, deployed anywhere in the world, with the communications needed to support the information dissemination and processing requirements.

It is essential that GCCS be capable of operating over tactical communication systems during power projection operations, and in locations where there is no DISN infrastructure available. GCCS uses a standardized infrastructure so that it can exploit new technologies. Since GCCS will not be developed and fielded as a single product, it was developed with the goal of facilitating the migration of existing systems into its COE. Essential capabilities operating in current systems will be maintained until those capabilities can be fulfilled in GCCS.

GCCS provides the common C<sup>2</sup> functions that a commander needs to fight effectively and win decisively. To meet these requirements, the system provides the trained personnel, procedures, reporting systems, communications, and automated information processing support for resolving the problems involved in developing an employment plan in a timely and effective manner. The employment plan provided the basis for developing the necessary mobilization, development, and sustainment planning requirements.

**1.2 Operational Performance Requirements.** In lieu of an ORD, the OEMP, OEP, J3/J6 message R132043Z Jun 94 and the CONOPS will constitute the complete requirements documents validated by the Joint Staff. The minimum acceptable operational performance requirements against which the GCCS fielding and WWMCCS shutdown (see the GCCS OEMP, Appendix F for IOC/WWMCCS Shutdown System Requirements) decision will be made when GCCS performs as well or better than the current WWMCCS environment and meets joint C2 requirements. GCCS success will be based on the user assessment of GCCS's ability to meet the

Joint Staff IOC requirements. The following MAOPRs are based on the requirements documents referenced above and the Joint Staff IOC requirements (establishing a network with robust connectivity, developing and fielding sufficient system architecture to support a redundant system that is not vulnerable to a single point of failure, migrating and integrating JOPES and other WWMCCS mission essential applications, fielding a top secret C2 system that supports top secret C2 requirements, providing the required number of trained personnel, identifying sufficient funding to operate and maintain the system). These MAOPRs were used to determine the critical operational issues identified in section IV of the GCCS OEMP. The following parameters will be measured during developmental and operational testing:

**1.2.1 WAN Infrastructure.** The WAN infrastructure provides compatibility to world wide router-based SIPRNET with the transfer rate being greater than or equal to 256 kps.

**1.2.2 Network Management.** The Network Management provides standards based Management Information Bases (MIBs) for monitoring the Relational Database Management System (RDBMS), operating system, and network segment operations.

**1.2.3 Remote Users.** The remote users support remote dial with the capability being greater than or equal to 4.8 kps. GCCS communications servers (CISCO 2511-CSs) are designed to support Secure Telephone Unit - III (STU-III) remote dial in, and low speed dedicated multiplexer circuits.

**1.2.4 Database Management.** Database Management provides FIPS 127 compliant RDBMS.

**1.2.5 Joint Operation Planning and Execution System (JOPES).** The JOPES Assessment Plan appendix B includes the critical functions to be tested for JOPES. GCCS shall be able to process an average of 7,000 transactions per day.

**1.2.6 Global Status of Resources and Training System (GSORTS).** GCCS application server shall support remote access and update of status of resources information. GSORTS data refresh up to 4MB in less than 2 Hours. GSORTS data reload up to 10MB in less than 4 Hours.

**1.2.7 Joint Deployable Intelligence Support System (JDISS).** JDISS provides on-site connectivity and interoperability with the intelligence systems required for Joint Intelligence Center (JIC), JTF, and operational commanders to execute the intelligence mission.

**1.2.8 Reliability, Maintainability and Availability Parameters.** The following are the reliability, maintainability and availability (RM&A) parameters as stated in the OEMP for GCCS, dated 10 October 1995.

**1.2.8.1 Site Reliability.** GCCS Site Mean Time Between Operational Mission Failures (MTBOMF) shall be defined at a later date. MTBOMF is defined as the mean GCCS site

operating time between operational mission failures which cause or could cause the inability to perform one or more GCCS mission essential functions.

GCCS site level MTBOMF will be computed using the standard MTBOMF algorithm defined in Army Material Command Pamphlet (AMC PAM) 70-11, as follows:

$$\text{MTBOMF} = \frac{\text{Total GCCS Site Operating Hours}}{\text{Total GCCS Site Operational Mission Failures}}$$

Total site operating hours is the sum of fully mission capable operating hours, and total operational mission failures is the total number of GCCS failure incidents, where total site operating hours is the sum of fully mission capable operating hours, and total operational mission failures is the total number of GCCS mission essential failure incidents.

**1.2.8.2 Component Reliability.** The GCCS component level Mean Time Between Failures (MTBF) shall be defined at a later date. Component MTBF is defined as the mean GCCS component operating time between failures. GCCS component-level MTBF estimates will be computed using the standard MTBF algorithm defined in AMC PAM 70-11, as follows:

$$\text{MTBF} = \frac{\text{Total GCCS Component Operating Hours}}{\text{Total GCCS Component Failures}}$$

Operations component failures are defined as those component failures for which corrective maintenance cannot be deferred.

**1.2.8.3 Maintainability.** GCCS Mean Time to restore software (MTTR<sub>sw</sub>) and GCCS Mean Time to repair hardware (MTTR<sub>hw</sub>). The MTTR failures shall not exceed 3 hours for hardware repair actions and 3 hours for software restore actions. These estimates will be revised at a later date and will be based on empirical data. MTTR is the measure of maintainability which describes the average active maintenance time required to complete unscheduled (corrective) maintenance and return a system or component to an operational state after the occurrence of a failure. MTTR is defined as the total active corrective maintenance clock time divided by the total number of corrective maintenance actions performed. Active corrective maintenance time includes the time required to restore all processes, functions, files and databases to a tactically useful state as well as the time to physically reboot the system and enable user logins. Active corrective maintenance time does not include travel time, logistics delay time or administrative delay time. Software failures are defined as any random interruption of the system's operation, other than those directly attributable to hardware, which can be restored to the pre-interrupted state.

GCCS MTTR estimates will be computed for mission operations failures, and hardware and software repair actions, using the MTTR computational algorithm defined in AMC PAM 70-11, as follows:

$$\text{MTTR} = \frac{\text{Total Active Corrective Maintenance Time}}{\text{Total Corrective Maintenance Actions}}$$

Software repair actions are defined as corrective actions taken to restore or reinitialize system operations to the point of processing in progress prior to software module failure. Software repair actions do not include off-line actions taken to revise or update software code.

**1.2.8.4 Availability.** Traditionally, availability has been calculated from a standpoint of hardware uptime and availability for the user to do work. The operational availability ( $A_o$ ) factor for each GCCS site will be derived from the RAM data collected by JITC designated data collectors at each IOC site. However, using the old paradigm approach, GCCS site  $A_o$  estimates would have been computed using the  $A_o$  computational algorithm defined in AMC PAM 70-11, as follows:

$$A_o = \frac{\text{OT/FMC} + \text{OT/DMC} + \text{ST}}{\text{OT/FMC} + \text{OT/DMC} + \text{ST} + \text{TPM} + \text{TCM} + \text{TADT} + \text{TLDT}}$$

Where:

OT/FMC	=	Total Operating Time/Fully Mission Capable
OT/DMC	=	Total Operating Time/Degraded Mission Capable
ST	=	Total Standby Time
TPM	=	Total Preventive Maintenance Downtime
TCM	=	Total Corrective Maintenance Downtime
TADT	=	Total Administrative Delay Downtime
TLDT	=	Total Logistics Delay Downtime

TPM and TLDT down times (for reasons other than awaiting spare parts) will not be included in the  $A_o$  computation for GCCS priority operations, as both represent deferrable downtime. TPM and TLDT down times would have been included in calculating  $A_o$  for GCCS routine operations.

The GCCS is fully mission capable if it is capable of performing all mission functions. The GCCS is degraded mission capable if it is not capable of performing one or more mission functions, but is capable of performing all mission essential functions. Using the current methodology above, an accurate reflection of mission readiness cannot be achieved for distributed information systems in general and GCCS in particular.

#### **1.2.8.5 GCCS Mission Operational Availability (GMOA) Measurement.**

Consider that the formula for  $A_0$  above (in paragraph 1.2.8.4) is based on old technology, where hardware and software and data were all stored in the same device. The system being replaced, WWMCCS, is based on mainframe technology. Either the user connected by a terminal is up/down or the mainframe is up/down. A user can move to another terminal or wait until the down terminal is repaired (some state of degraded mission capable). When the mainframe is down, all users are affected and the site mission cannot be accomplished in its entirety (not mission capable). In the past, rather than being concerned about mission effectiveness, hardware up/down time was measured as a percentage of total time and not as the ability of the site user to perform the mission. The following paragraphs provide a different paradigm for measuring operational availability.

It may be added that GMOAs will be derived from the empirical data on Reliability, Availability, and Maintainability (RAM) collected by JITC designated data collectors at the GCCS IOC sites during the 45 days of the User Assessment. Site-level MTBOMF and Time to Restore estimates will be derived from the collected RAM data. GCCS IOC configuration does not support calculation of component level MTBF or MTTR at present.

**1.2.8.5.1 Background.** Consider the new environment for the Global Command and Control System (GCCS). In the open system, client server environment, the “site” needs to be viewed from a hardware standpoint as the Database Server, the Applications Server(s), and the User Client workstation. These devices are connected by Communications Paths. From a software standpoint, Applications Software is loaded in segments across the hardware continuum. It is necessary from a Systems Viewpoint to consider that a Mission Function is the composite of software, data segments, and connectivity required in a distributed system.

Therefore, Availability should be considered in more than a hardware up/down paradigm.

#### **1.2.8.5.2 GCCS Mission Operational Availability (GMOA) Measurement.**

There are 11 Mission Areas described in the GCCS Mission Need Statement (MNS). For the implementation of each Mission Area, there are software segments and data that must be available to the user. In Appendix E, a narrative discussion and a spreadsheet of a sample site outlines this philosophy in real terms.

Software Segments	Mission Areas										
	MA1	MA2	MA3	MA4	MA5	MA6...	MA11				
SW1	X		X								
SW2		X		X	X						
SW3				X		X.....	X				

The sites shall assign the 11 mission areas with weights from 0 to 10, where 0 indicates that the absence of that mission area does not affect the site. An assignment of weight 10 to a mission area indicates relative priority of work performed and the necessary redundancy required both in user client workstations and software segments on multiple application servers.

The general case is now described as:

This leads to a definition of GMOA that states the following:

For “Site 1” and “Mission Area 1”, “Software Segment 1” is very important and must be available from 5 client workstations or “Seats.”



“Mission Area 2” and thus “Software Segment 2” is less important and needs to be available from 2 “Seats” only.

“Mission Area 11” is not important at this site and there is no impact if it is not available, even though it is available at one seat.

Sites shall ensure that the number of workstation clients is equal to or greater than the number required for a mission area.

### 1.2.8.5.3 Mathematical Definition of GMOA Measurement.

GCCS Mission Operational Availability ( $A_o$ ) at a specific site  $(Site)_n$  is as follows:

$$A_o(Site)_n = 1 - \sum_{i=1}^N \left\{ 1 - A_o(SCF)_i \right\} - \frac{\sum_{i=1}^M a_i \left\{ \left[ 1 - A_o(MCF)_i \right] + \left[ 1 - \frac{\sum_{j=1}^{K_i} A_o(WSF)_{i,j}}{K_i} \right] \right\}}{\sum_{i=1}^M a_i}$$

Definitions:

$A_o(Site)$  The overall system mission operational availability on a site basis.

$A_o(SCF)_I$  The system operational availability due to system critical failures which bring down the entire site (i.e. failure of the premise router).

$N$  The number of possible critical failures which could bring down an entire site.

$M$  The number of mission areas supported by GCCS.

$\alpha_i$  The relative importance on a scale of zero to ten for the I-th mission area supported by GCCS at that particular site.

$A_o(MCF)_I$  The system operational availability due to failures (other than workstations or application servers) of system elements necessary to support mission area “I”.

$K_i$  The number of workstations required to support the “I-th” mission area.

$A_o(WSF)_{ij}$  The operational availability due failures which cause the loss of work position “j” (either due to workstation or application server failures), if those failures cause the number of available work positions to drop below the number required ( $K_i$ ) for mission area “T”.

The only other caveat is that simultaneous failures between  $A_o(SCF)_i$  and mission area failures cannot be counted separately.  $A_o$  can be decremented only once for such simultaneous failures. Likewise, simultaneous failures between  $A_o(MCF)_i$  and workstations cannot be counted separately.  $A_o$  will be decremented only once for such simultaneous failures.

### **1.3 System Support Risks**

**1.3.1 Funding.** Funding for operations and support of GCCS must be budgeted by DISA and the Services as directed in the Defense Planning Guidance. Life cycle management and funding policy is still in its early stages of development.

**1.3.2 Network Management.** Use of two separate network management systems for GCCS and the Top Secret Support System (TS3), increases the risk in the area of network management. The Top Secret Support System (TS3) is a separate network and does not interface with GCCS. There is an initiative to acquire and implement a network management software tool to perform software configuration management and version control. Without such a tool, there is a risk that untested and/or non-approved software may interfere with or contaminate the GCCS system.

**1.3.3 Training.** Training availability must keep pace with the COE evolution while simultaneously being able to expand and contract according to a rapidly changing world mission. Training is being developed concurrent with the design of the system.

**1.3.4 Post Deployment Software Support.** Legacy system changes, new development software, and logistics support for Government off-the-Shelf (GOTS) software are issues which need to be addressed in developing this support strategy. Procedures related to system change initiation, management, testing, and implementation are in coordination and will be defined to cover the life cycle of system changes and be in accordance with CJCSI 6721.

**1.3.5 Hardware and Software Maintenance.** Fielding to date has included hardware and software delivered to sites both in the Continental United States (CONUS) and Outside the Continental United States (OCONUS). Planning for the maintenance is being accomplished in parallel with the field level implementation planning. Thus Services and Sites may not have adequate time to develop appropriate detailed support plans and budgets prior to fielding.

**1.3.6 Software Tailoring and Configuration Management.** The GCCS PMO and the sites must maintain strict engineering and configuration control of the system to minimize the potential for

degradation of GCCS.

## **2. MAINTENANCE CONCEPT**

The DISN backbone up to but not including the premise router is a DISA support responsibility. The premise router up to and including the GCCS hardware is a Service/site support responsibility. DISA funded, for DISA fielded hardware, an initial period of maintenance to allow the Services and sites to plan and budget for their life cycle support concepts. For all sites, this coverage will end 30 June 1996. Services will provide hardware and software maintenance support to their host sites beginning 1 July 1996. GCCS hardware and operating system software at DISA supported sites will be maintained by contractor support for the life cycle of the system. Sun Silver Service will be used initially, to be followed by the DISA GCCS Maintenance Contract upon award in March 1996. Each Service/Agency (S/A) responsible for supporting GCCS sites has developed a tailored support concept. When provided, S/A-specific information is included for each area discussed in this JILSP.

**2.1 Air Force.** The Air Force is developing a two-level maintenance concept with a mix of organic and contractor maintenance at both organization and depot level, depending upon deployment requirements. The DISA GCCS Maintenance Contract is available for Air Force use.

**2.2 Army.** The STCCS PMO intends to utilize the DISA GCCS Maintenance Contract, when awarded, for hardware maintenance after March 1996. In the interim, Life Cycle Contractor Support (LCCS) will be the primary means of maintenance for system and applications software and all hardware [ADP Equipment (ADPE) and communication] being fielded under the auspices of AGCCS. Users will conduct only limited system diagnostics. Maintenance will be provided under the purview of existing LCCS maintenance contracts whenever possible. Maintenance, which is outside the scope of existing LCCS contract, will be satisfied under separate maintenance contracts managed by the STCCS PMO.

**2.3 Navy.** The Navy intends to use the DISA GCCS Maintenance Contract to support all shore sites for the life of the contract. For all shipboard units with the installed TAC-n series hardware, maintenance will continue to utilize the procedures currently in place. All software maintenance for the Navy's service unique mission applications are the responsibility of the Navy and will be implemented in accordance with the configuration management policy and procedures.

**2.4 Marine Corps.** USMC will establish a maintenance concept that indicates the requirements for both garrison and deployed site system restoration [i.e., the exchange of Line Replaceable Units (LRUs) with contracted LRU repair and the use of deployment kits in lieu of contractor support while in a deployed status]. In addition to contract maintenance support, the Marine Corps must have the capability to provide limited maintenance (replacement of LRUs) without voiding the maintenance contract or warranty. The use of diagnostic software and deployment kits (consisting of recommended spares) may be required in lieu of contractor support. USMC will address Military Occupational Specialty (MOS) specialty codes for other than operator (9919 MOS) to meet specific

Marine Corps requirements. They will also discuss what maintenance action is accomplished at each echelon of maintenance as well as how MCTSSA plans to be a focal point for forwarding failure/deficiency reports to DISA. The detailed USMC maintenance concept will be provided in the User's Logistics Support Summary. The DISA GCCS Maintenance Contract is available for Marine Corps use.

### **3. LOGISTICS SUPPORT ANALYSIS**

A Logistics Support Analysis (LSA) was not conducted for the GCCS program.

### **4. ACQUISITION STRATEGY**

GCCS acquisitions will use existing contracts and special purpose limited scope acquisitions. This approach provides flexibility to utilize either the Services or industry as maintainers of products.

To accomplish this the Migration Director will use existing DISA, the Services, large contractors, or Small Disadvantaged and Minority Owned Businesses as acquisition vehicles for evolving the functional capabilities of the GCCS.

A primary source of contractual services to support the GCCS Migration will be the Defense Enterprise Integration Services (DEIS), awarded by DISA in late 1993. This set of six contracts provides a strong source of expertise for the integration and migration services needed for GCCS.

Delivery orders to DEIS teams will be the major avenue for providing new contractual services to DISA in FY94 and FY95.

Contractual efforts already underway will be examined and adjusted to fit into the overall GCCS migration. Maximum use will be made of existing contracts to support the overall migration strategy within the levels of currently defined funding.

All acquisition efforts under GCCS will be based on the rapid development of manageable pieces of the overall environment. Large and lengthy development efforts will be avoided. Significant additions to the GCCS environment will be acquired over time. These additions will be partitioned into modules that can be delegated to multiple agencies. These modules would be developed in coordination with the others and integrated into the Common Operating Environment of the GCCS program.

The vision for the GCCS migration does not fit neatly into the traditional milestone reviews set forth for a major weapon system acquisition. The "waterfall" method for software system design, frequently found in such large programs, provides a poor structure for the management of the integration and migration envisioned to establish the GCCS environment.

**4.1 Life Cycle Cost (LCC) Reduction Actions.** The following methods will be employed to reduce

or control LCC to include acquisition and operation and support (O&S) costs, using existing standardized components where possible.

- Acquiring COTS equipment and software
- Employing GOTS equipment and software
- Reusing software where possible
- Building toward common systems
- Competitively awarded hardware and maintenance contract

## **5. TEST AND EVALUATION CONCEPT**

**5.1 Integrated Test Program Schedule.** The GCCS test and evaluation strategy is designed to leverage the development efforts of a large number of programs. Each program may have several development organizations. GCCS includes the integration of CINC and Service-unique applications which have to be integrated before GCCS user exercises can be run. In addition, the Service-unique operational data sets must be transferred from WWMCCS into the GCCS application databases. Other applications will be integrated as they become available. GCCS will employ an incremental integration, test and fielding approach. Target application requirements identified by the functional proponent will be segmented, tested, and fielded. The T&E strategy will utilize developmental and operational test and evaluation methods described in sections three and four respectively. DT&E will be performed by the software support activities, the GCCS integration contractor and DISA. OT&E will be performed by the JITC in conjunction with the Service test agencies (AFXO/ACC, OPTEC/OEC, OPTEVOR, MCTSSA) (JITC). The operational assessment of the early versions of GCCS is being conducted by the user community under the auspices of the Joint Staff (J3). Additional assessments of CINC and Service unique applications integrated into GCCS will be done by the providing CINC or Service and supplemented by independent operational tests.

**5.1.1 Developmental Test and Evaluation.** The objectives of the developmental test and evaluation are to determine whether the systems under test meet the technical/specification requirements and to reduce the risk of an adverse impact when inserting new products and technology into the operational system. GCCS releases will undergo computer software unit, component, and configuration item testing by the development contractor. System integration, installation, multi-node, integrated system, and version testing will be performed by the integration agency in concert with the user.

**5.1.1.1 Test Facilities.** Test facilities include the Operational Support Facility (OSF) in Sterling, VA; the Joint Demonstration and Evaluation Facility in Arlington, VA and the Joint Interoperability Test Command (JITC) test bed at Fort Huachuca, AZ. Each of these facilities maintain GCCS operating platforms, software, and communications equipment necessary to operate as an operational GCCS site with remote access to the various CINC and Component GCCS sites worldwide. Each facility is able to support test case development, system performance analysis, joint exercises, GCCS

user workshops, and other system demonstrations. These facilities provide the capability to balance testing done in the laboratory with that expected in the operational environment.

**5.1.2 Operational Evaluation.** The purpose of the GCCS Operational Evaluations (OE) is to demonstrate the extent to which the GCCS meets the operational needs of the users from the NCA to JTF commanders in providing an interoperable, fully integrated C4I systems for the warfighter. The list of OE critical short term issues relate to GCCS IOC and WWMCCS shutdown. The preliminary critical operational issues are in the areas of performance, interoperability, security, survivability, sustainability, manpower and personnel integration, WWMCCS shutdown, and COE. As part of the JITC's Continuous Comprehensive Evaluation (CCE) approach, data will be collected in an incremental manner to reduce risk and provide opportunities for early user feedback. Data collected will support decisions on fielding software and on WWMCCS shutdown.

**5.2 Interoperability Certification.** The Joint Interoperability Test Command (JITC) is responsible for certifying that the GCCS complies with applicable standards and meets requirements for interoperability, compatibility and integration. This certification is presented to the GCCS Program Manager (PM), the appropriate Office of the Secretary of Defense (OSD) T&E Offices and the Chairman of the Joint Chiefs of Staff (JCS). The JITC will participate in ongoing GCCS test efforts to ensure interoperability capabilities are appropriately addressed and to monitor the contractor's compliance with the Joint Interoperability Engineering Organization (JIEO) approved GCCS Standards Profile. In coordination with the operational evaluation (OE), JITC interoperability evaluators will monitor and collect data during all available data collection opportunities. JITC evaluators require access to design documentation and system design reviews to facilitate the Continuous Comprehensive Evaluation (CCE) and Interoperability Certification process. The JITC will perform or witness all GCCS testing activities using the CCE method and assist the GCCS PM as required in conducting and evaluating all aspects of the GCCS program. The JITC will report results of independent operational tests to the Director of DISA, DOT&E and JCS/J3. The interoperability evaluation will address GCCS external interfaces in the following priority:

- (1) Systems and databases that GCCS must interface with to perform JOPES and other WWMCCS mission essential functions.
- (2) Systems and databases that GCCS must interface with to perform new GCCS functions.
- (3) Systems and data bases that GCCS must interface with to perform CINC/Service/JTF/Command-unique functions. CINC/Service/JTF/Command-unique functions that are critical to WWMCCS shutdown will be given the highest priority in the interoperability evaluation effort.

**5.3 Test and Evaluation Management Responsibilities.** Management responsibilities for the GCCS program are as follows:

a. ASD (C3I). Support the organizational coordination on the GCCS Test and Evaluation strategy.

b. DOT&E. Responsible for the final approval of coordinated OEMP and OEPs. Also responsible for the oversight of test planning and conduct and independent evaluation and reporting of GCCS performance.

c. DTSE&E. Reviews development test results to analyze residual risks and satisfaction of entrance criteria.

d. JITC. Responsible for the following activities:

- (1) Independent operational testing
- (2) Interoperability testing and certification
- (3) Coordination with Service test communities to leverage test planning, conduct, and evaluation of Service-unique critical mission tasks
- (4) Site installation evaluation
- (5) Consolidating the reporting on meeting entrance criteria requirements
- (6) Writing the OEP and serving as the single test integration point of contact
- (7) Test training and coordination
- (8) Control over the GCCS configuration during the operational phase of testing, and control over access by contractors that might alter the configuration
- (9) Ensure that all critical mission tasks are performed and evaluated, or that the consequences of not performing any critical mission are assessed by the affected users as an acceptable risk and test limitation
- (10) Consolidate evaluation reports from appropriate sources; conduct, analyze, and evaluate the joint portion of GCCS operational testing; and reporting test results directly and simultaneously to the Joint Staff, Director of DISA, and DOT&E with information to the Services.

e. DISA/GCCS Integration Office. Responsible for the following activities:

- (1) Complete the description of the transition strategy options for fielding and backing up the GCCS both before and after IOC. DISA will provide version description documents, system administration procedures and a cutover plan for the database and long haul communications.
- (2) Provide baseline and developmentally tested software and related support to IOC sites according to the "Global Command and Control System Fielding Criteria" (J-6A 01290-94, October 1994).
- (3) Complete the development test of the Common Operating Environment (COE).

f. Services. Responsible for the following activities:

- (1) The specification and approval of the operational requirements and operational procedures for Service unique elements of GCCS
- (2) Conduct operational test and evaluation for Service unique mission critical capabilities in support of the OEP and appended Service test plans. Operational test support includes writing test plans, test execution, evaluating test results and providing the evaluation of operational effectiveness and suitability to JITC for consolidation into the overall GCCS evaluation. This will allow JITC to monitor Service unique testing prior to IOC.

g. Joint Staff. Responsible for the following activities:

- (1) The specification and approval of operational requirements, specifically up to IOC, in lieu of an ORD via a letter of transmittal and its attachments
- (2) Conduct a threat assessment for GCCS in accordance with DoD 5000.2
- (3) Final approval authority for the operational use of GCCS and conventional WWMCCS ADP termination.
- (4) Represent the CINCs for the OEMP and OEP.

h. Users at CINCs and Sites. Responsible for the following activities:

- (1) Provide to the J-3 and JITC CINC/site unique test plans or test process descriptions that are deemed critical/essential to the evaluation of GCCS and support the WWMCCS shutdown decision.
- (2) Support the test process as directed in the coordinated OEMP. It may include conducting the tests planned by the CINC/sites, permitting JITC observation if necessary, and reporting results to the JITC for consolidation.
- (3) Help collect and report data including JITC questionnaires and support tester's adjudication processes for evaluating problems.

**5.3.1 Army.** Testing will be accomplished IAW DoDI 5000.2 and AR 73-1. The overall AGCCS program test strategy is currently being developed and will be approved by the AGCCS Test Integration Working Group (TIWG). The USA Electronic Proving Grounds (EPG) will conduct Independent Developmental Testing (IDT) of the AGCCS. The USA Operational Test and Evaluation Command/Operational Evaluation Command (OPTEC/OEC) will provide Operational Assessment (OA) of the AGCCS products as they are installed and tested at program milestone/decision points.

## **6. ILS ELEMENTS**

This section describes how the GCCS PMO plans to incorporate the elements of ILS into the development and fielding of the system. For each ILS Element discussed, Service-specific detail



is included where provided by the appropriate Service(s). Service support concepts vary and therefore, not all sections include information for each Service.

**6.1 Maintenance Planning.** Maintenance planning is the process of establishing a maintenance concept and support requirements for a system's life cycle. The GCCS will be maintained by contractor support initially for all DISA provided hardware. DISA supported sites will be maintained by contractor support for the life cycle of the system. For all other sites, follow-on support may be acquired through the DISA GCCS Maintenance Contract (to be awarded by 30 June 96), or any other available support option deemed appropriate by the S/A supporting the site. The purpose of the DISA Maintenance Contract is to provide a contractual vehicle should it be required by any S/A, to obtain GCCS maintenance. The S/A providing support to each GCCS site will be responsible for providing funds to satisfy both hardware and operating system software maintenance requirements for the life cycle of the system. The GCCS Customer Management System/Hotline serves as the entry point for any GCCS functional, technical, configuration and software questions and/or problems requiring further research and analysis.

**6.1.1 Customer Management System/Hotline.** The initial point of entry for any questions and/or problems, will be to the DISA customer management system Hotline. The DISA customer management system consists of a 24-hour, 7 day/week Hotline; a call tracking system; and a Global System Problem Report (GSPR) Form tracking system. The Hotline serves as the entry point for any GCCS functional, technical, configuration and software questions and/or problems requiring further research and analysis. Every call received by the Hotline is logged and used for the collection of systems integrity data and for action tracking. A GSPR can also be initiated through the Hotline for software problems requiring software modifications and/or enhancements. Callers will be directed to the specific vendor hotline or maintenance source, as applicable, by DISA customer service. Calls will be referred to or coordinated with, the individual Service hotlines when it has been determined that Service unique equipments and/or procedures are affected. The 24-Hour Hotline telephone numbers are:

Comm:	(703) 735-8681
DSN:	653-8681
FAX:	653-8685

Between the hours of 1800-0600 Monday-Friday, the call will be forwarded to DISA staff personnel. All day Saturday, Sunday and holidays the call will be answered by the DISA Hotline voice mail message system. The voice mail system will direct the caller as to what actions should be taken depending upon the priority of the requirement.

**6.1.2 Interim Hardware Maintenance Concept.** The following hardware maintenance concept will be used by all DISA supported sites and most Service supported sites, until the DISA Maintenance Contract is available. The callers to the Hotline will be referred to the appropriate maintenance activity and should not contact the agencies directly.

**6.1.2.1 Sun Hardware and Solaris Operating System Software Maintenance.** Sun hardware and Solaris operating system software (procured by DISA) will be fielded with a short-term maintenance contract agreement, usually for one year. Maintenance period funded by DISA, will vary depending on date of hardware purchase and shipping periods. This maintenance will be furnished by Sun or a vendor as Sun Silver Service. Features include: 24-hour telephone assistance, with optimum coverage from 8AM Eastern to 8 PM Pacific, Monday- Friday; on-site service within 24-hours; replacement hardware parts with the on-site technician; Solaris enhancement releases; patches and maintenance releases; a Sun-Solve license; and Sun Early Notifier Service, which provides answers to most frequently asked customer questions. Sites may identify the priority of their call as Urgent, Serious, or Non-critical. These priority designations will dictate the level of response required from the contractor. Urgent will receive live transfer telephone assistance with a 4-hour on-site response time. Serious will receive a 2-hour telephone call-back with a next-day (24-hour) on-site response time. Non-critical will receive a 4-hour telephone call-back with on-site response at customer convenience. Any OCONUS location outside a 50-mile radius of a SunService office, will be supported on a best-effort basis, within 24-hours for on-site response. Every effort will be made to respond to urgent priorities on the same day the call is received. To report a hardware or operating system software problem for equipment covered under the Sun maintenance contract, the site system administrator must contact Sun Corporation's Hotline number directly.

This agreement will not cover replacement of secure disks. Sites will be required to supply a replacement disk for any secure disk repair. DISA will make available to sites spare disks to support repair of secure disks until the GCCS maintenance contract is awarded in March 1996. The DISA GCCS maintenance contract will include maintenance and replacement of secure disks.

**6.1.2.2 CONUS Maintenance Support.** CONUS sites may access Sun maintenance after being directed to do so by the DISA Hotline, by calling Sun directly at: 1-800-USA-4-SUN; (1-800-872-4786) while the Sun Silver Service Agreement is in place. Sun has two telephone SunService Centers in the United States, one on the east coast and one on the west coast. The centers are staffed 24 hours a day, but are staffed most heavily during the hours of 8AM to 8PM. Therefore, the optimum coverage availability is between the hours of 8AM Eastern and 8PM Pacific. Call routing is determined by loading. Once the call has been answered, the SunService Center Operator will request the following information:

- Company Name (DISA/your site)
- Site Phone Number
- Local Contact
- System Serial Number
- System Model Number
- Sun Schedule/ Maintenance Contract Number:
- Application software version
- Solaris release

- Description of problem

**6.1.2.3 OCONUS Maintenance Support.** Telephone service is available 24 hours a day, as described in paragraph 6.1.2.1 above. Optimum coverage is available from 8:00 A.M. Eastern to 8:00 P.M. Pacific. Sites should only contact Sun after being directed to do so by the DISA Hotline.

Sites should use the applicable local phone number listed below, (or if none is listed, the CONUS number identified in para 6.1.2.1):

Germany:	0130-81-5377
Guam:	To Be Determined (TBD)
Japan:	TBD
Korea:	0038-11-0048
Panama:	011-800-872-4786
UK:	0800-96-3828

The SunService Center Operator will request the following information:

- Company Name (Service, Location, Agency)
- Site Phone Number
- Local Contact
- System Serial Number
- System Model Number
- Description of Problem (Be specific)
- Sun Schedule/ Maintenance Contract Number: (SCXXXXXX)

Any OCONUS location outside a 50-mile radius of a SunService office, will be supported on a best-effort basis, within 24-hours for on-site response. Every effort will be made to respond to Urgent Priorities on the same day the call is received.

Refer to the site-specific MFP or ULSS for a list of equipment at specific sites, the appropriate maintenance contract information, and the maintenance coverage expiration date.

**6.1.2.4 FDDI Hub and Lan Concentrator Maintenance.** Maintenance for the FDDI Hub, Lan Concentrator, and Hub Router, is provided through the PRC Super-Minicomputer Contract, F19630-93-D-0001. An initial twelve month warranty period comes with the procurement of each system. Follow-on maintenance needs to be procured by the Services beginning 1 July 1996. These three equipments are Core equipments as defined in the contract. The warranty period is 9-hour On Call Principal Period of Maintenance (OCPPM) 0800-1700 local time, Monday through Friday, except Federal Holidays. This is true for both CONUS and OCONUS installations. For CONUS installations, the required "Time to Repair" is 4 OCPPM hours for

Core components and 24 OCPPM hours for OCONUS installations. The DISA Hotline should be contacted before attempting to go to the vendor directly. For specific information on this contract, refer to the Super-Minicomputer Contract User Guide, Release February 1995. Copies of this document will be made available to sites. Sites should call the GCCS Customer Management System/Hotline for assistance in obtaining support under this contract. See paragraph 6.1.1 for detailed description of Hotline and phone numbers. The toll-free number for the PRC Customer Response Center (CRC) is 1-800-852-MINI (1-800-852-6464).

**6.1.2.5 Top Secret Support System (TS3) Hardware Maintenance.** TS3 is a completely separate and stand-alone system from GCCS. It contains the top secret data and applications which was previously on WWMCCS. The following paragraphs describe the maintenance concept for the TS3 components.

**6.1.2.5.1 Network Encryption System (NES).** DISA funded a five year extended maintenance agreement for the NES in November 1994. To report symptoms of malfunction and for shipping instructions, contact Motorola Customer Service at (602) 441-3449. Customer Service will provide a Return Materials Authorization (RMA) for authorized repair. NES trained users will have a PIN for calling in a NES failure. The serial number on the devices can also be used. Shipments should be coordinated with the Comsec Custodian and contain the following: details of the problem; DD1149 or packing list; list of all part numbers and serial number of hardware returned; and, site point of contact name and phone number. The government funds the shipping to Motorola. The same item will be repaired and returned within an estimated 2 to 4 week time frame.

**6.1.2.5.2 CS2600 Server.** DISA funded a one year maintenance agreement in November 1994, which is being renewed for Fiscal Year 1996. This agreement requires the initial contacting of customer service to report symptoms and receive shipping instructions. Customer service will issue shipping instructions and an RMA for authorized repair after being provided: Model Number (CS2600) and serial number; diagnostic failure symptoms; and Delivery Order Number. Return shipment will include: device only (no cables, s/w or documentation), carefully packed; diagnostic printout; and printed RMA number on outside of box. The government pays for shipping to the vendor. A 2 week turn-around time can be expected. Spare CS2600 Servers are located in Hawaii (1), OSF (2) and Stuttgart (1). To report symptoms of malfunction and to receive shipping instructions, the following customer service activities should be contacted.

<u>Location</u>	<u>Company</u>	<u>Phone Number</u>
CONUS	3COM	(800) 876-8763
CONUS & Pacific	3COM	(408) 492-1790
Europe	European Repair Service	+44 442 278125

**6.1.2.5.3 Unitec UT-200.** DISA funded a one year maintenance agreement in November 1994,

which is being renewed for Fiscal Year 1996. This agreement requires the initial contacting of Thomas Engineering Customer Service to report symptoms and receive shipping instructions. The CONUS customer service number is (800) 832-8649 and for OCONUS (510) 938-2920. Customer Service will issue shipping instructions and an RMA for authorized repair after being provided: Model Number (CS2600) and serial number; diagnostic failure symptoms; and Delivery Order Number. Return shipment will include: device only (no cables, s/w or documentation), carefully packed; diagnostic printout; and printed RMA number on outside of box. The government pays for shipping to the vendor. Spare Unitec Ut-200's are located at the Pentagon, FCDNA, and ANMCC. A 3-5 day turn-around time can be expected.

**6.1.2.5.4 STU 1910 SAC.** AT&T Customer Service should be contacted at (800) 243-7883, to report symptoms of malfunction and to receiving shipping instructions. An RMA will be issued upon the receipt of the Model Number (STU 1910) and serial number. A replacement STU will be shipped upon receipt of the trouble call. Return shipments should include the printed RMA number on the outside of the box. The government pays for shipping to the vendor. DISA is not funding STU III maintenance.

**6.1.2.6 SAT Maintenance.** The Automated Message Handling System (AMHS) Standard Automated Terminal (SAT) is supported through three methods. The sites should always initially contact the DISA Hotline before contacting any vendor. The CCP-2 boards have an initial 90 day warranty. DISA has procured an annual software maintenance agreement through FY-96 for 37 sites from Cavalier Communications, Inc. at (703) 758-7900. The Sun PC-NFS 5.1 Single User 163-3135 Media and Documentation, Sun PC-NFS 5.1 Single User 163-3137 License and Sun PC-NFS 5.1 Single User Software Maintenance are supported through Sun. The Compaq Deskpro 450's and Magnavox monitors were procured from AmeriData with warranties of three years. OCONUS activities are required to deliver the monitors to an authorized service provider. For Deskpro warranty service, the Compaq Technical Support Center at 1-800-652-6672 or AmeriData Systems at (301) 258-9737. Monitor warranty service is available from AmeriData Systems at the above number.

**6.1.2.7 Premise Router Maintenance.** Premise router maintenance is the responsibility of the S/A and/or site. DISA is in the process of negotiating the addition of GCCS premise router maintenance to the Defense Data Network (DDN) Hardware/Software Services Contract, DCA 200-91-C-0002. The S/A and/or sites will be able to procure maintenance for the premise routers in the same way they currently procure maintenance for their other routers and network devices through this contract. The DDN contract is a Defense Business Operating Fund (DBOF) contract. The GCCS Maintenance contract will be a source of maintenance for the premise routers, when awarded in June 1996. Sites should call the GCCS Customer Management System/Hotline for assistance in obtaining support under this contract.

**6.1.3 Long Term Hardware Maintenance Concept.** The long term maintenance concept for GCCS hardware and operating system software for DISA-supported sites is contract

maintenance. S/A supported sites will be maintained as deemed appropriate by the responsible S/A. The DISA GCCS Maintenance Contract will be open to use by S/As. The contract will offer a variety of maintenance support options from which S/As may select those most appropriate for their sites. S/As have funding responsibility beginning FY96. Options include extensions to principle periods of maintenance (9 hours, 0800-1700, Monday through Friday) from 9 to 24 hours with response times of 2, 4, 8, and 24 hours. Remedial, preventive, per-call, on-site, crisis, and exercise maintenance provisions will be addressed in the contract. Further details will be provided after contract award in March, 1996.

**6.1.4 Software Maintenance.** Maintenance of GCCS PM-procured COTS software provided to IOC sites will be funded by DISA through 30 September 1996. The COTS software life cycle management and support concept, to include funding for software licenses and maintenance, is still being defined. The Joint Staff is responsible for licensing guidance and any subsequent changes to it. Services/sites will provide any additional COTS licenses required above the quantity provided by DISA, and will be responsible for maintenance of these licenses as well. DISA is investigating a purchasing vehicle whereby sites will be able to obtain additional software. Information regarding procedures will be forwarded via Autodin message when available. Updates to GCCS joint service applications are the responsibility of the respective Government Executive Agency. The Executive Agency may periodically update and enhance an application and submit that changed application to the GCCS PM and GCCS System Engineer for review for acceptance into GCCS.

**6.1.4.1 Software Problem Reports and Engineering Changes.** GCCS users may submit problem reports and suggested engineering changes. At present, each problem report is being submitted as a GSPR to the GCCS Hotline or to GCCS Configuration Management. At some point in the future, the GCCS Hotline will receive all GSPRs. Electronic submission is preferred. A "Known Errors" list is provided with each system or application fielding. The list consists of significant problems encountered by DISA integration testing or problems reported by the sites. The "Known Errors" list will not contain any priority 1 or 2 items as defined by MIL-STD-498, Appendix C. Methodologies for accomplishing GSPRs are explained in the various Version Description Documents, the Configuration Management (CM) Plan, and other documents and instructions. CM Policy is being rewritten by JCS (J36). Engineering changes may be submitted as a GSPR by the same methods. Problem reports and engineering changes will be analyzed and acted on as appropriate.

**6.1.4.1.1 Army.** GCCS problem reports will be directed to DISA through the AGCCS Help Desk and EBB.

**6.1.4.1.2 Marine Corps.** USMC problem reports will be directed to DISA via MCTSSA and not directly from individual USMC sites. USMC Configuration Control Board members will be addressed in the ULSS.

**6.1.4.2 Commercial Software Products.** Commercial software products required for GCCS will be distributed centrally by the GCCS PMO. This software is limited to that necessary for execution of the various GCCS applications. It will generally be distributed with the pertinent application or system.

**6.1.4.3 Software Licenses.** Some COTS software licenses are being procured by DISA on an Enterprise basis. Site licenses and user licenses are provided when hardware is fielded. Life cycle software management policy which is still TBD, will dictate whether Services must also procure and maintain some licenses. DISA will employ a software license management tool to monitor site license usage. Configuration of COTS software products will be centrally managed by DISA. Refer to your site-specific maintenance support document, MFP or ULSS for software licensing information pertaining to your particular site.

**6.1.4.4 Software Maintenance Funding.** Maintenance for DISA procured COTS software licenses will be funded through FY96. Future software maintenance for both DISA-provided COTS licenses and for any additional COTS licenses procured by the Services/sites must be funded by the Services.

**6.1.5 Warranties.** DISA accepted the Sun option to up-lift the warranty on hardware and operating system software to a maintenance agreement. This will provide for a period of maintenance from the date of system acceptance and allow the S/A time to plan and budget for maintenance coverage. The period of performance and type of coverage are discussed in paragraph 6.1.2 above. The FDDI Hub, Lan Concentrator, and Hub Router warranties are for twelve months beginning with acceptance by the Government. The twelve month warranty covers all parts, labor, upgraded software, and limited telephone support. The FDDI Hub, Lan Concentrator and Hub Router are considered "core" items and have a four CONUS and twenty-four hour OCONUS principle period of maintenance repair times. Principle period of maintenance is calculated on an eight hour day, Monday through Friday except for federal holidays. The Premise Router warranty covered an initial period of 90 days. All Premise Routers are now outside the warranty period and are no longer covered by warranty.

**6.2 Personnel.** Each Service is responsible for preparing a manpower assessment and reviewing their training requirements. Current WWMCCS billets are the primary source for GCCS system operations personnel at most commands. However, since GCCS is more than a WWMCCS replacement, locations will not be able to draw upon WWMCCS personnel without first providing new GCCS specific training to these personnel. Warfighters, planners and other GCCS users will be located within existing Service staffs. These personnel also will need GCCS training. As additional functions and capabilities are added to GCCS, the manpower requirements will be constantly migrating to meet the changing support environment.

**6.2.1 Site Manpower Requirements.** There are seven specific duties and job titles which

comprise the "GCCS on-site team." For specific training requirements for these positions refer to the Air Education and Training Command (AETC) GCCS Training Plan. The following provides a brief description of the requirements for the "GCCS on-site team."

**6.2.1.1 GCCS Site Coordinator (GSC).** Responsible for coordinating all system and network support activities within the GCCS site. This individual filling this role will be the primary focal point for coordinating with the GMC and other GCCS organizations. One of the major duties of this position will be to direct activities during and following an emergency condition to minimize the loss of GCCS mission capabilities at the site. For large organizations, the site commander or DAA may want to appoint additional personnel in this function. They will be referred to as an Assistant GCCS Site Coordinator (AGSC). This position was previously known as the WIN Site Coordinator.

**6.2.1.2 GCCS Network Administrator (GNA).** Responsible for the day-to-day operation of the GCCS LAN are the data and applications servers, the communications devices (premise router, communications server, and intelligent hubs), and related GCCS equipment. Duties include:

- Maintain the Local Area Network (LAN)
- Maintain the AUTODIN/DMS (future) interface
- Identify and be capable of installing each LAN component
- Maintain the LAN system interface
- Operate the LAN
- Troubleshoot network and communications problems
- Maintain applicable TEMPEST and physical security requirements
- Provide expertise in TCP/IP services

This position was not formally recognized within the WWMCCS environment though most WWMCCS sites had maintenance personnel performing this function.

**6.2.1.3 GCCS System Administrator (GSA).** Responsible for a variety of duties with the major focus being on maintaining the GCCS applications, providing local user support, and troubleshooting site problems associated with the GCCS applications. This includes the responsibility of determining if the GCCS applications are properly storing correctly formatted data to the GCCS database servers. Duties include:

- Direct activities during and following an emergency condition to minimize the loss of GCCS mission capabilities at the site
- Maintain access permission lists
- Maintain the Executive Manager permissions program
- Add and remove hardware and software at the local site



- Perform system startups and backups
- Generate periodic summaries of system performance and utilization
- Routinely backup data and audit files
- Setup user accounts and passwords
- Coordinate database modifications with other site personnel and the GMC-Pentagon
- Diagnose system problems and report them to the GSC and GMC-Help Desk

A thorough understanding of the GCCS COE and software philosophies will be instrumental in accomplishing the duties of this position. This new position most closely matches the WWMCCS position that was previously held by the senior Functional Manager (FM) at a WWMCCS site.

**6.2.1.4 GCCS Database Administrator (GDBA).** Responsible for the day-to-day operations of the databases located at the GCCS site. This may include the primary database server (SUN Sparc 1000 or Sparc 2000) running the Oracle RDBMS, or the Executive Manger application using the Sybase RDBMS, or the AMHS server application using the Verity Topic RDBMS. If the GCCS site does not have any of these databases this position may be vacant. The Duties include:

- Coordinate incremental/ backups of the databases with the GSC and GMC Pentagon
- Generate periodic summaries of database performance and utilization
- Coordinate and maintain database modifications
- Monitor all database applications for proper performance
- Manage disk/tape storage

This position most closely matches the WWMCCS position that was previously known as the Technical Database Manager (TDBM).

**6.2.1.5 GCCS Site Designated Approving Authority (GCCS Site DAA).** Responsible for local security policies and guidance to ensure the integrity and security of the GCCS operations is maintained. Receives direction and guidance from the Joint Staff GCCS DAA. These duties will be similar to those performed by the Site DAAs who supported WWMCCS.

**6.2.1.6 Site GCCS Security Officer (SGSO).** Responsible for ensuring the integrity and security of the local GCCS system and network. This position was previously known as the WASO.

**6.2.1.7 GCCS System Support Programmer (GSSP).** Responsible for providing support to the GCCS System Administrator to maintain the GCCS applications, provide local user support, and troubleshoot site problems. In addition to the duties outlined for the GSA, the GSSPs will

have additional duties to fulfill. These duties are the following:

- Monitor total system performance to ensure optimal performance
- Reconfigure GCCS to regain processing capabilities for non-routine equipment malfunctions
- Assist users in determining the cause of failures
- Prepare training material and train site personnel
- Maintain system and application configuration parameters
- Maintain GCCS applications

Again, understanding of the GCCS COE and software philosophies will be instrumental in accomplishing the duties of this position. Most sites may have multiple personnel filling this role as each person will have different areas of technical expertise. This position most closely matches the WWMCCS positions that was previously held by the Functional Database Managers (FDBMs).

**6.2.2 Service Personnel Requirements.** Each Service has manpower projection models which are used to project manpower requirements based upon a set of parameters that are peculiar to that Service and its mission. From these models, other analyses, and operational experience each Service will determine whether any special service or qualification codes (i.e. Navy Enlisted Code (NEC), Air Force Specialty Code (AFSC), MOS, etc.) are required to identify and assign GCCS qualified individuals. Service unique training requirements will be identified and/or tailored for Service unique requirements.

**6.2.2.1 Air Force.** Air Force Regulation (AFR) 25-5, "Air Force Management Engineering Program (MEP) Policies, Responsibilities, and Requirements" provides guidance and methodology for determining manpower requirements. The MEP is the basic approach to manpower planning and programming for the Air Force. The MEP relies on the application of various tools and techniques to determine manpower requirements. These include, but are not limited to: conventional manpower standards, mathematical models, the Logistics Composite Model (LCOM), minimum manpower/staffing patterns, Standard Indirect Allowance Factors (SIAFs), and directives [e.g., base operating support (BOS) factors]. Any or all of these may be used to determine the quality and quantity of manpower required to perform or support the work of the functions being studied. The parent command has final responsibility for the manpower requirements determination process, for many systems.

**6.2.2.2 Army - Manpower and Personnel Integration (MANPRINT).** Manpower and personnel refers to the identification and acquisition of military and civilian personnel with the skills and grades required to operate and support the material system over its lifetime. MANPRINT is the Army process of integrating the full range of human factors engineering, manpower, personnel, training, health hazard assessment, and system safety to improve personnel and total system performance throughout the material development and acquisition process.

MANPRINT purpose is to influence systems' designs so that developmental and non-developmental items are operated and maintained in the most cost effective and safest manner consistent with manpower structure, personnel, aptitude and skill, and training resources of the Army. The AGCCS System MANPRINT Management Plan (SMMP) details the system's MANPRINT objectives, responsibilities, and issues. DA and DoD proponents use the SMMP to analyze the Project's adherence to the seven domains of MANPRINT: manpower, personnel, training, human factors engineering and analysis, health hazards, system safety and soldier survivability. The AGCCS sites use the SMMP to identify site MANPRINT issues and actions.

**6.2.2.3 Navy.** The HARDMAN program provides the procedures and methodology to facilitate manpower requirements analysis early in a new weapon system acquisition. As implemented by OPNAVINST 5211.7, "Determining Manpower, Personnel, and Training (MPT) Requirements for Navy Acquisitions," the military manpower/hardware integration (HARDMAN) program provides the necessary tools, techniques, and methodology for identification of MPT concepts and resource requirements for any acquisition program from program initiation through fleet introduction. OPNAVINST 5310.22, "Navy Manpower Engineering Program (NAVMEP) Policy" consists of five sub-programs used in planning, programming, and budgeting for manpower resources to support the Navy's operating forces and shore establishments.

**6.2.2.4 Marine Corps.** The Marine Corps uses the Navy's models and manages its manpower requirements and projection from Headquarters, U.S. Marine Corps.

**6.3 Supply Support.** There is no plan to provision spares to support GCCS hardware. The DISA GCCS maintenance contract offers a source of contract maintenance service to include all required spares and repair parts. Until the contract is awarded (by 1 March 1996), DISA will make available to Sites a limited number of spare disks to support repair of secure disks.

**6.3.1 Provisioning.** The system will not be provisioned. The contractor as part of the GCCS Maintenance Contract is required to furnish spare and repair parts as part of their maintenance. There may also be a requirement to identify and pre-position spares to support contractor maintenance and repair for some sites. These decisions are Service unique.

**6.4 Support Equipment.** Support equipment includes all equipment (mobile or fixed) required to support the operation and maintenance of a system. No unique GCCS support equipment has been identified. For all equipment maintained under the DISA GCCS Maintenance Contract, the contractor will be responsible for providing any support and test equipment necessary to maintain the equipment at the level required by the contract.

**6.5 Technical Data.** Technical data is recorded information of a scientific nature, and includes the manuals, drawings, parts lists, change notices, system software documentation, and other technical publications related to the operation and support of a system. Documentation of computer programs and related software are technical data; however, the actual computer

programs and related software are not. Technical data also includes specifications, standards, engineering drawings, task analysis instructions, data item descriptions, reports, and equipment publications. Table 1 contains a list of GCCS Documentation provided the Sites with Release 2.1.

**Table 1 - GCCS Version 2.1 Documentation**

<b>DOCUMENT #</b>	<b>DOCUMENT TITLE</b>
LL-210-06-02*	JDISS Computer System Reference Manual
LL-210-08-02*	JDISS Security Concept of Operations
LL-211-01-01	JMCIS (Joint Maritime Command Information System) Handbook
LL-211-10-01	JMCIS 2.1.System Administrators Guide
LL-211-11-01	JMCIS 2.1.Security Managers Guide
LL-500-102-04*	GCCS Version Description Document
LL-500-103-14*	GCCS 2.1 Implementation Procedures for Automated Information Systems
LL-500-13-02	GCCS Block 1 User Handbook
LL-500-133-01*	GCCS System Users Manual: GCCS Version 2.1
LL-500-147-03	GCCS Ad Hoc Query User Manual with Change Pages Inserted
LL-500-29-05*	GCCS System Administration Manual for GCCS Version 2.1
LL-500-43-04*	GCCS Sys/Security Implementation Instructions for SSA
LL-500-67-04*	GCCS Automated Information System (AIS) Security Plan
LL-501-11-01	UCCS(AMHS)System Administrator/Operator Guide
LL-501-12-03	UCCS EUCOM DSS/BS-AMHS Workstation User Guide
LL-504-02-03	TARGET Users Manual (Draft)
LL-505-03-02	GSORTS User's Guide
LL-505-18-01	GSORTS FRAS Users Manual
LL-507-01-02	MEPES (Medical Planning and Execution System) Core Users Manual (UM)
LL-509-03-02*	RDA (Requirements Development and Analysis)Build 2 Users Manual
LL-516-03-01*	RUDRS Version Description Document
LL-517-04-02*	PREDEFINED Reports Users Manual
LL-518-05-03*	GRIS CSCI v2.2 Operators Manual with Change Pages Inserted
LL-521-05-01	Airfields Software Installation Plan
LL-521-07-02	Airfields Software Users Manual

LL-521-11-01	Airfields Software Center Operator Manual
LL-522-00-03	FRAS (Fuel Resource Analysis System)Known Problem List
LL-522-02-01	FRAS (Fuel Resource Analysis System) Installation Instructions
LL-522-03-01	FRAS (Fuel Resource Analysis System) Operators Manual
LL-527-02-01	LEGENT System Manager Agent Release 2.1.0 Release and Installation Notes
LL-527-03-01	LEGENT System Manager Release 2.1.0 Users Guide
LL-527-05-01	LEGENT DB Agent for Oracle Release 1.0.0 Notes and Installation Notes
LL-527-06-01	LEGENT DB Manager Release 1.0.0 Users Guide
LL-527-07-01	LEGENT DB Agent for Oracle Release 1.0.0 Reference Manual
TL-128-08-01	EVAC User Manual
TL-162-06-08	LOGSAFE Software Users Manual (SUM)
TL-194-01-03	JFAST 6.0Users Guide (UG)
TL-198-03-02*	DART Users Manual Build 3.4
TL-199-23-08	TIP Technical Administrators Manual/GCCS System Administrator's Manual
TL-201-27-03	S&M Client/Server Software Users Manual with Change Pages Inserted
TL-202-01-04	JEPES (Joint Engineer Planning and Execution System) Users Manual
NA-000-00-001	Topic Database Administrators Guide V.3.1, Vol.1
NA-000-00-001	Topic Database Administrators Guide V.3.1, Vol.2
NA-000-00-001	Topic Real -Time Administrators Guide V4
TBD	JOPES User's Guide
TBD*	GCCS System Reference Guide
NA-000-00-002	ORACLE Database System Administrator Manual

\* Available in digital

**6.5.1 User's Manuals.** All GCCS system level documentation will be provided in hard copy at the time of initial installation of the system at a GCCS site. This consists of any system administration manuals, GCCS user's guides, specific application user's manuals, software installation procedures, and limited commercial manuals. The commercial manuals provided are the standard manuals provided by the vendor to any customer. These manuals are limited to hardware and operating system user's manuals and vendor repair locations/phone numbers.

**6.5.2 Maintenance Manuals.** Since all GCCS hardware is standard commercially available equipment and will be maintained by contractor support, no maintenance manuals are provided to

GCCS sites.

**6.5.3 Operations Manuals.** Subsequent major updates of software and new application deliveries will include changed or new operations manuals as available.

**6.5.4 DISA/JIEO Configuration Management Department Library.** A master copy of government produced GCCS documents and software which have been provided for CM library control, is maintained by the DISA/JIEO Configuration Management Department library. The library provides one copy of available documentation at the time of fielding, as discussed above. It is the responsibility of each GCCS site to reproduce the documents as necessary if multiple copies are needed. Single, replacement copies may be requested from the CM library, at the following numbers: Commercial: (703) 735-8732 or DSN prefix: 653. A library of commercial manuals is not maintained. Additional copies of commercial manuals must be requested by the site from the appropriate vendor. Publication changes will be provided to each site by the CM library. Changes will be in the form of change pages or complete documents.

**6.5.5 Publication Updates.** Sites may submit recommended publication updates and changes to GCCS documents via Global System Problem Reports (GSPR), DISA Form 291. This should be accomplished via the GCCS Hotline. This form can be produced using the "FormFlow" commercial form filler package. DISA Form 291 is available on the DISA LAN in FormFlow. The electronic template of the form is available from the DISA/JIEO Configuration Management Division. It is preferred that completed forms be submitted electronically whenever possible.

**6.5.6 Reprourement Data Package.** A reprourement data package is not being procured with any of the systems. The systems will not be re-competed in the traditional scenario but will consist of independent but integrated COTS/GOTS packages within the overall system. These independent packages provide a function which is integrated into the overall system. This allows only the function to be competed and not specific actions or interfaces.

**6.5.7 Classified Data.** All documentation and software, when initially delivered to the sites, is marked as UNCLASSIFIED. Upon installation onto the SECRET-level GCCS system, the software and tape cartridges become SECRET, and must be handled accordingly. Cartridges may be downgraded if proper downgrade procedures for electronic media contained in CSC-STD-005-85, are followed. Classified technical publications will be classified in accordance with Service requirements and marked in accordance with DoD 5220.22M and MIL-M-38784. Classified data and publications handling will be accomplished in accordance with CSC-STD-005-85, "Department of Defense Magnetic Remanence Security Guideline."

**6.6 Training.** The DISA GCCS ILS Manager (D423) is the GCCS Training Manager. A Memorandum of Agreement dated 8 August 1994 between Joint Staff J3, J6 and HQ USAF/SC assigned the Air Force as the technical Single Service Training Manager (SSTM) for GCCS. All technical training activities are coordinated through AETC. All functional training activities are

coordinated through JTO. The GCCS SSTM is responsible for determining contents of GCCS courses and developing a technical Training Plan for GCCS. This agreement takes advantage of the existing WWMCCS training resources to rapidly develop and deploy GCCS technical training. The JOPES Training Organization (JTO) develops and provides GCCS functional applications training. The purpose of the GCCS JOPES transition and migration training is to prepare joint warfighters at the Unified and Specified Commands and at CINC component levels. The Training Course Plans and Schedules for GCCS technical and functional training are independent documents. The current versions of these training course catalogues are listed in Appendix B of this JILSP.

**6.6.1 GCCS Training Master Plan.** DISA's GCCS PMO is developing the GCCS Training Master Plan. The DISA GCCS ILS Manager (D423) is responsible for coordinating GCCS training. The ILS Manager ensures the correct numbers of courses are developed scheduled and that GCCS personnel are trained to meet and support GCCS operational requirements.

**6.6.2 AETC Training Plan.** The AETC GCCS Training Plan serves as the reference for GCCS technical training courses. This plan is a consolidated document which contains the policies and procedures for the GCCS technical training program. In particular, it contains the training methodology, student training categories, mobile training team support requirements, course descriptions, training points of contact and the responsibilities of various activities involved in GCCS technical training.

**6.6.3 JOPES Training Organization Course Catalog.** The JOPES Training Organization Course Catalog provides a mission description of the JOPES Training Organization, brief course descriptions, and schedules of each GCCS functional course offered. JOPES training points of contact are also listed in the JTO Course Catalog.

**6.6.4 Training Concept.** The GCCS training program is supported by military, government civilian and contractor instructors. These resources are employed to conduct training at AETC located at Keesler Air Force Base (AFB), MS, the JTO located at Scott AFB, IL and the AETC Detachment located at the OSF in Sterling VA. GCCS sites can use Mobile Team Training (MTTs) when made available by AETC and JTO. GCCS technical and functional training augments the on-the-job training provided during site installation and provides a continued source of training to meet skill and knowledge requirements and attrition. The GCCS users need to know how to operate in the COE. This COE is the baseline which the SSTM and JTO are using to consolidate their training efforts.

**6.6.4.1 Technical Training.** AETC, the SSTM located at Keesler AFB, MS, manages all resources for GCCS technical training. This includes system administration, database administration, security administration, operating systems, and user training on operations and some functional applications of the COE. The COE is the infrastructure of GCCS, providing platform services and support applications such as e-mail, teleconferencing, message handling,

word processing and spreadsheets, as well as providing access to the core software applications.

**6.6.4.2 Functional Training.** JTO, located at Scott AFB is the single functional training manager responsible for developing and providing GCCS functional training for planning and execution related mission applications. The functional training gives the GCCS users with hands-on training for mission applications. The mission applications are Requirements Development Analysis (RDA), which was called Dynamic Analysis and Replanning Tool (DART) in WWMCCS, and Joint Operation Planning and Execution System (JOPES) Basic Operations Course, which was called JOPES Migration during FY95 under WWMCCS. Effective FY96 Scheduling and Movement (S&M) will not be taught as a separate course but has been incorporated into the JOPES Basic Operations Course. Force Augmentation Planning and Execution System (FAPES) and Logistics Sustainment Analysis and Feasibility Estimator (LOGSAFE) functional training are also offer by JTO. The JTO functional course catalog is updated semiannually or as required by JTO.

**6.6.5 Training Methods.** Training will be provided via one of the following three methods.

**6.6.5.1 Resident Training.** This is where students are sent to the instructors at a centralized training facility. AETC will use current facilities at Keesler AFB MS, and their detachment at DISA's OSF in Sterling, VA to provide resident training. Additionally, the JTO at Scott AFB, IL will provide resident training on JOPES.

**6.6.5.2 Mobile Training Teams (MTTs).** MTTs will be sent to either regional training facilities or to host sites capable of providing a classroom environment. MTTs are traveling instructors who go to the students' site and provide training in either an on-site or regional training facility. It is anticipated that this type of training will be provided on a regularly scheduled basis as required by the sites.

**6.6.5.3 Interactive Courseware (ICW).** The SSTM is planning to use a certain number of host servers as ICW servers, linking them together through a web-browser program such as Mosaic. When the user accesses the ICW icon on the screen, they will get a Home Page identifying courses available. Pointing and clicking on a specific course will bring that course on-line for the user, or download it to their machine to run as a resident program. Student registration screens will be available for those students wishing to receive credit for taking the course. ICW is an all inclusive term that includes Computer Assisted Training (CAT) or Computer Based Training.

**6.6.6 Courses of Instruction.** The creation, development, modification of courses is a continuous and on-going effort as GCCS matures and additional capability is added to the system. Course length and content is modified whenever it is determined that changes are needed to meet the operational user needs. Courses are constantly being added, modified, and updated to support fielding of GCCS. For these reasons, the most current course catalogs from AETC and JTO should be consulted prior to the scheduling of training. The course catalogs and points of contact



are listed in Annex B.

**6.6.6.1 Funding for Training.** DISA provides funding to AETC for GCCS course development and presentation of training. JTO is funded by USTRANSCOM's Defense Business Operating Fund (DBOF) T fund. Effective FY96 the Joint Staff no longer funds AETC and JTO directly. Funding from the Joint Staff Program Element was transferred to DISA beginning 1 October 1995. DISA will provide funding to AETC for sustainment training after IOC. TRANSCOM will fund the JTO for sustainment training. Temporary Duty (TDY) costs for students are the responsibility of the respective command, service, or agency receiving the training. These TDY costs include student transportation and lodging. Funding for MTT instructors is the responsibility of AETC and JTO. Organizations sending students to MTT locations are responsible for funding the students' TDY costs.

**6.6.7 Sustainment Joint Training Strategy.** After IOC, all courses listed in paragraph 6.6.6 will continue to be taught. The individual services are responsible for developing their Service unique GCCS training plans and extended GCCS training requirements.

**6.6.7.1 Army AGCCS Training Site (ATS).** The ATS, Fort Gillem, Georgia provides AGCCS modernization training to Army site users. USTRANSCOM uses the ATS as a regional training facility on a quarterly basis to provide GCCS and JOPES training. The STCCS PMO has the overall responsibility to resource, manage, and operate the ATS to coordinate training requirements with the sites. The ATS plans, schedules, and conducts modernization training. The ATS manager, with contractor support, is responsible for developing, implementing, and maintaining training for key site personnel. Due to funding constraints, the sites will maximize the use of Computer Based Training (CBT) and Embedded Training (ET), when possible, to satisfy sustainment training of their remote sites. The ATS is responsible for developing and propagating CBT/ET pertaining to Army specific subjects. The ATS is also responsible for developing the CBT/ET so that it is accessible through the GCCS WAN. The sites will use the products to supplement other training resources. OCONUS training locations may be formally established at a later date.

**6.7 Facilities.** Facilities are the permanent, semi-permanent, or temporary real property assets required to support the system. The facilities required for GCCS initial fielding, depending on a site's proposed configuration, should accommodate either a SUN Sparc 1000 Data Server (with two disk expansion pedestals) or a Sun Sparc 2000 Data Server and three SUN Sparc 20 Application Servers. The SUN Sparc 1000 (Configurations C2, C3, and C4) Data Server and SUN Sparc 20 Application Servers can reside in a regular office environment/facility. The Sun Sparc 2000 Data Server and Sun Sparc 1000 (C1) Data Server requires a raised floor environment/facility.

Facilities to support follow-on fieldings will be described in respective site MFP/ULSS. A site survey is performed prior to the hardware/software installation on each proposed GCCS site to

ensure that the GCCS COE facility and utility requirements are addressed and met.

**6.7.1 Utility Requirements.** The utility required for the GCCS COE, depending on a site's proposed configuration, should accommodate either a Sun SPARCserver 1000 (with two disk expansion pedestals) or a Sun SPARCcenter 2000 and three Sun SPARCserver 20 computers in a facility meeting the respective fielding facilities requirements.

**6.8 Packaging, Handling, Storage and Transportation.** There are no system unique packaging, handling, and storage requirements for unclassified GCCS hardware or software. Items are packaged for transportation by commercial or military, surface, or air transport. Guidelines are found in MIL-STD-129L and MIL-STD-794E. No special test requirements, or depot considerations are required other than those contained in the referenced guidelines.

**6.8.1 Storage Modes.** All GCCS version release components being shipped to the proposed GCCS sites are UNCLASSIFIED and should be treated as such for storage. Upon installation onto the SECRET-level GCCS system, the software and tape cartridges become SECRET, and must be handled accordingly. The fielding facility can be used as the storage area for any equipment received prior to the arrival of the installation team. If at any instance, classified material is shipped for a specific GCCS version release, storage of the classified material should be performed using the sites' standard operating procedures for storing classified material in secure areas.

**6.8.2 Transportation and Transportability.** The GCCS components are transportable via normal transportation procedures and safeguards for ADP equipment.

**6.8.2.1 Shipping Requirements.** All GCCS version release components being shipped to the proposed GCCS sites are UNCLASSIFIED and should be treated as such. Upon installation onto the SECRET-level GCCS system, the software and tape cartridges become SECRET, and must be handled accordingly. Military air shipping services will be used for routine shipments. Priority shipments will use other government approved shipping services. If at any instance, classified material is shipped for a specific GCCS version release, they will be marked and shipped appropriately. Packaging of GCCS equipment for shipment will be IAW MIL-STD-129M (15 Jun 93) "Marking for Shipment and Storage - (Part 1 of 4 Parts)," MIL-STD-2073-1B (21 Jun 91) "DoD Material Procedures for Development and Application of Packaging Requirements (Part 1 of 2 Parts)," and MIL-STD-2073-2C (21 Jun 91) "Packaging Requirement Codes (Part 2 of 2 Parts)."

## **6.9 Design Interface**

**6.9.1 Reliability, Availability, and Maintainability (RAM).** A key design interface of the GCCS is the Joint operational and technical requirements. The GCCS must ensure the system meets Joint criteria and parameters of RAM and other Joint Required Operational Capability

(JROC) criteria, and the system is interoperable and compatible with other Service GCCS systems.

**6.9.2 Standardization.** The GCCS design shall accommodate the common C<sup>2</sup> requirements of all CINCs, Services, and agencies, as well as accommodating the DoD Intelligence Information System (DODIIS) requirements for interoperability and integration purposes. The GCCS, through its common operating environment, will provide the identical look and feel to all users, maximizing its use while reducing training and maintenance requirements. The Software Design Document for the Global Command and Control System (GCCS) Concept of Operations should be referenced for additional information on standardization.

**6.9.3 Commonality.** The GCCS hardware platforms shall support the Transmission Control Protocol/Internet Protocol (TCP/IP), Government Open Systems Interconnection Profile (GOSIP) when requirements dictate and associated TAFIM standards.

**6.9.4 Interoperability.** A higher degree of interoperability can be achieved through the implementation of a well-aligned, standards-based Open System Environment (OSE). The use of Information Technology (IT) standards will provide an effective interoperation between new systems, and provide a migration path for future interconnections in an OSE.

GCCS standards guidance is based on adherence to the DoD TAFIM. In particular, Volume 7 of the TAFIM includes the OSE standards recommendations entitled "Adopted Information Technology Standards (AITS)." The AITS defines the target groups of standards to be used in new implementations.

In addition to the TAFIM, MIL-STD-187-700 "Interoperability and Performance Standards for the Defense Information System" shall be used to promote interoperability of DoD telecommunications systems. It contains the technical standards and design objectives needed by both the strategic and tactical users. It provides for the digital exchange of all forms of information.

GCCS will use the DISN for most backbone communication services and CINC JTF communication assets for other communications needs. Many remote Air Force locations are going to be connected to GCCS using the Air Force Command and Control Network (AFC2N) with crossover points to the SIPRNET.

Future releases of GCCS must be interoperable with:

- DISN
- The Defense Message System (DMS)
- The DODIIS Corporate Network

- The DODIIS Corporate Network Joint Worldwide Intelligence Communications System (JWICS)
- The GTN acquisition effort
- Interface with site infrastructure: (TBD)
- Inter-service support requirements: (TBD)

**6.9.5 Security.** GCCS will be implemented and operated as a SECRET high system. Multi-Level Security (MLS) is part of the GCCS objective plan, and it will be upgraded as new capabilities become available.

**6.9.6 Links.** A GCCS network will be established using the DISN. The network routing system will be configured to preclude single points of failure. Bandwidth will be provided to meet routine operational commander's information requirements.

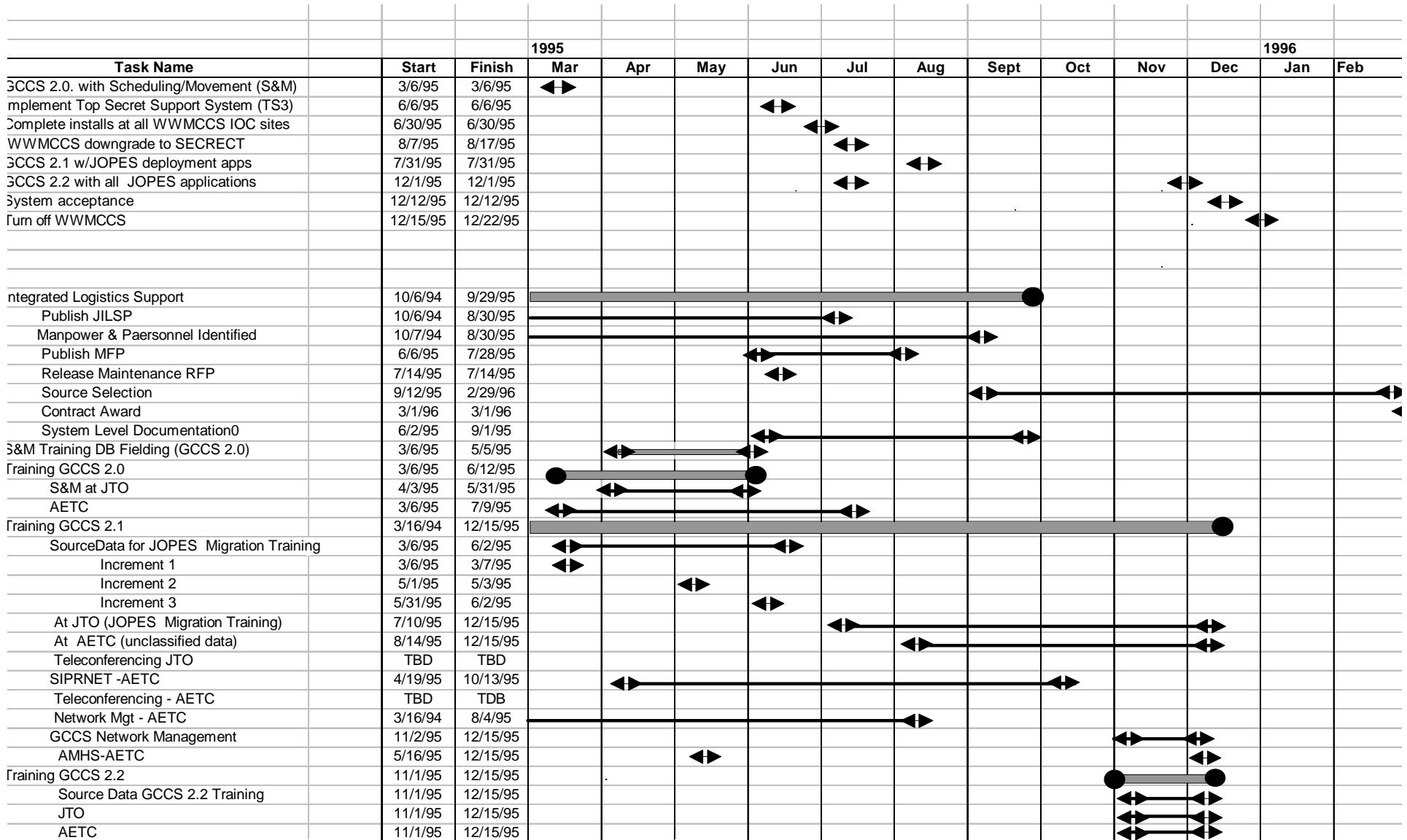
**6.9.7 Availability.** GCCS is being designed to meet the performance parameters reflected in Part II, paragraph 1.2.

**6.9.8 Information Priority.** Information flow is controlled by the combination of "push" and EEI data inputs. In the event of a contingency, unexpected congestion, unusual demand levels or damage to the system, the GCCS network control can take actions to maximize system availability to predefine critical users.

**6.9.9 Flexibility.** The GCCS design shall permit rapid expansion or contraction of client support at locations in addition to modifications of software for enhanced service. Deployable assets shall have mobility features equal to the supported command structure.

**6.9.10 Compatibility.** Common data elements will be used when re-engineering existing systems or applications.

## PART III - MILESTONE SCHEDULE



#### **IV. FIGURES, TABLES and ANNEXES**

Figures 1, 2 and 3 are found on pages 5, 6, and 10, respectively. Table 1 is found on page 27 and Table 2, on page 39. The Annexes A, B, and C follow.

**ANNEX A**  
**GLOSSARY OF ABBREVIATIONS AND ACRONYMS**

**A**

ADP	Automated Data Processing
ADPE	ADP Equipment
AETC	Air Education and Training Command
AFB	Air Force Base
AFC2N	Air Force Command and Control Network
AFR	Air Force Regulation
AFSC	Air Force Specialty Code
AGCCS	Army Global Command and Control System
AGSC	Assistant GCCS Site Coordinator
AITs	Adopted Information Technology Standards; Advanced Information Technology Services
AMC PAM	Army Material Command Pamphlet
AMHS	Automated Message Handling System
A <sub>o</sub>	Operational Availability
APML	Assistant Program Manager for Logistics
AR	Army Regulation
ARCOM	Army Reserve Commands
ARPA	Advanced Research Projects Agency
ASD	Assistant Secretary of Defense
ATS	AGCCS Training Site
AUX	Apple UNIX

**B**

BOS	Base Operating Support
BPS	Bits Per Second

**C**

C <sup>2</sup> / C2	Command and Control
C <sup>3</sup> /C3	Command, Control, and Communications
C <sup>3</sup> I/C3I	Command, Control, Communications, and Intelligence
C <sup>4</sup> I/C4I	Command, Control, Communications, Computers, and Intelligence
CAT	Computer Assisted Training
CBT	Computer Based Training
CCE	Continuous Comprehensive Evaluations
CD ROM	Compact Disk - Read Only Memory

CFI	Center for Integration
CINC	Commander in Chief
CISC	Complex Instruction Set Computer
CIS	Command Information System
CISS	Center for Information System Security
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	CJCS Instruction
CJTf	Commander, Joint Task Force/ Combined Joint Task Force
CM	Configuration Management
CMO	Configuration Management Office
CNO	Chief of Naval Operations
COE	Common Operating Environment
Comsec	Communication Security
CONOPS	Concept of Operations
CONUS	Continental United States
COTS	Commercial-off-the-Shelf
CPU	Central Processing Unit
CRC	Customer Response Center
CS	Communications Server
C/S	Client/Server
CTAPS	Contingency Theater Automated Planning System
CTAPS (ATO)	Contingency Theater Automated Planning System (Air Tasking Order)

## D

DA	Department of the Army
DAA	Designated Approving Authority
DART	Dynamic Analysis and Replanning Tool
DBOF	Defense Business Operating Fund
DDA	Designated Development Agent
DDN	Defense Data Network
DEIS	Defense Enterprise Integration Services
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMC	Defense Mega Center/ Degraded Mission Capable
DMS	Defense Message System
DoD	Department of Defense
DODI	DoD Instruction
DoDIIS	DoD Intelligence Information System
DOS	Disk Operating System



DSN	Defense Switched Network
DT	Development Test
DT&E	Development Test and Evaluation

## E

EBB	Electronic Bulletin Board
EEI	Essential Elements of Information
EPG	Electronic Proving Grounds
ELINT	Electronic Intelligence
EST	Eastern Standard Time
ET	Embedded Training

## F

FAPES	Force Augmentation Planning and Execution System
FDBM	Functional Database Managers
FDDI	Fiber Distribution Data Interface
FIPS	Federal Information Processing Standards
FMC	Fully Mission Capable
FSP	Facility Support Plan

## G

GB	Gigabyte
GCC	Global Command and Control
GCCS	Global Command and Control System
GDBA	GCCS Database Administrator
GIPSY	Graphic Information Presentation System
GMC	GCCS Management Center
GMOA	GCCS Mission Operational Availability
GNA	GCCS Network Administrator
GOSIP	Government Open Systems Interconnection Profile
GOTS	Government off-the-Shelf
GSA	GCCS Systems Administrator
GSC	GCCS Site Coordinator
GSORTS	GCCS Status of Resources and Training System
GSPR	Global System Problem Report
GSSP	GCCS System Support Programmer
GTN	Global Transportation Network

## **H-I**

HARDMAN	Hardware and Manpower
HP	Hewlett Packard
IAW	In Accordance With
ICW	Interactive Courseware
IDS-1	Integrated Database Store (the database manager on DPS8)
IDT	Independent Developmental Testing
ILS	Integrated Logistics Support
ILSM	ILS Manager
ILSMT	ILS Management Team
ILSO	ILS Officer
ILSP	Integrated Logistic Support Plan
ILSMT	ILS Management Team
IMC	Integrated Management Centers
IMP	Interface Message Processor
IMRAS	Individual Manpower Requirements and Availability System
IOC	Initial Operational Capability
IP	Internet Protocol
ISO	International Standards Organization
IT	Information Technology
ITSG	Information Technology Standards Guidance

## **J**

J3	Director of Operations, Joint Staff
J6	Director for Command, Control, Communication and Computer Systems
	Joint Staff
JCS	Joint Chiefs of Staff
JDEF	Joint Demonstration and Evaluation Facility
JDISS	Joint Defense Intelligence Support System
JFAST	Joint Flow and Analysis System for Transportation
JIC	Joint Intelligence Center
JIEO	Joint Interoperability Engineering Organization
JILSMT	Joint Integrated Logistics Support Management Team
JILSP	Joint Integrated Logistics Support Plan
JITC	Joint Interoperability Test Command
JMAS	Joint Missions Application Software
JMCIS	Joint Maritime Command and Information System
JOPEs	Joint Operations Planning and Execution System
JPEC	Joint Planning and Execution Community
JROC	Joint Required Operational Capability

JPL	Jet Propulsion Laboratory
JTF	Joint Task Force
JTO	JOPEs Training Organization
JWICS	Joint Worldwide Intelligence Communications System

## K - L

kps	Kilo-bytes per second
LAN	Local Area Network
LCC	Life Cycle Costs
LCCS	Life Cycle Contractor Support
LCOM	Logistics Composite Model
LOGSAFE	Logistics Sustainment Analysis and Feasibility Estimator
LRU	Line Replaceable Unit
LSA	Logistics Support Analysis

## M

MAGTF	Marine Air Ground Task Force
MAJCOM	Major Commands
MAISRC	Major Automated Information System Review Committee
MANPRINT	Manpower and Personnel Integration
MAOPR	Minimum Acceptable Operational Performance Requirements
MARCORSYSCOM	Marine Corps Systems Command
MC	Marine Corps
MCEB	Military Communication Electronics Board
MCO	Marine Corps Order
MCTSSA	Marine Corps Technical Software Support Activity
MDW	Military District Washington
MEP	Management Engineering Program
MFP	Material Fielding Plan
MIB	Management Information Bases
MLS	Multi-Level Security
MNS	Mission Need Statement
MOBSTA	Mobilization Stations
MOP	Memorandum of Policy
MOS	Military Occupational Specialty
MPT	Manpower, Personnel and Training
MS DOS	Microsoft Disk Operating System
MTBF	Mean Time Between Failure
MTBOMF	Mean Time Between Operational Mission Failure
MTT	Mobile Team Training/ Mobile Training Teams

MTTR	Mean Time To Repair
MTTR hw	Mean Time To Repair Hardware
MTTR sw	Mean Time To Restore Software

## N

NATO	North Atlantic Treaty Organization
NAVMEP	Navy Manpower Engineering Program
NCA	National Command Authorities
NEC	Navy Enlisted Classification
NES	Network Encryption System
NOC	Network Operations Center
NOFORN	No Foreign
NSC	National Security Council

## O

O&O	Operational & Organizational
O&S	Operation and Support
OA	Operational Assessment
OC	Objective Capability
OCPPM	On Call Principal Period of Maintenance
OCONUS	Outside the Continental United States
OE	Operational Evaluations
OEC	Operational Evaluation Command
OEMP	Operational Evaluation Master Plan
OEP	Operational Evaluation Plan
OPNAVINST	Chief of Naval Operations Instruction
OPR	Office of Primary Responsibility
OPTEC	Operational Test & Evaluation Command
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OSE	Open System Environment
OSF	Operational Support Facility
OT	Operational Test/Operating Time
OT&E	Operational Test & Evaluation
OT/DMC	Total Operating Time/ Degraded Mission Capable
OT/FMC	Total Operating Time/ Fully Mission Capable

## P

PE	Program Element
----	-----------------

PHS&T	Packaging, Handling, Storage and Transportation
PMD	Program Management Documentation
PM	Program Manager
PMO	Program Management Office
PMW	PM Warfare
PO	Project Office
POM	Program Objective Memorandum
POSIT	Profiles for Open Systems Internetworking Technologies
PPBS	Planning, Programming and Budgeting System
PSL	Project Support Logistics

## Q-R

RAM	Reliability, Availability, and Maintainability/ Random Access Memory
RCC	Regional Control Center
RDBMS	Relational Database Management System
RFP	Request for Proposal
RM&A	Reliability, Maintainability and Availability
RMA	Return Materials Authorization
ROC	Required Operational Capability

## S

S/A	Services and Agencies
S&M	Scheduling and Movement
SA	System Administration
SAIP	Spares Acquisition Integrated with Production
SAT	Secure AUTODIN Terminal/ Standard Automated Terminal
SDP	System Decision Paper
SE&I	Systems Engineering & Integration
SGSO	Site GCCS Security Officer
SIAF	Standard Indirect Allowance Factors
SIPRNET	SECRET Internet Protocol Router Network
SMC	System Management Center
SMMP	System MANPRINT Management Plan
SOF	Special Operations Forces
SORTS	Status of Resources and Training
SPAWAR	Space and Naval Warfare Systems Command
SQL	Structured Query Language
SRO	System Readiness Objectives
SSTM	Single Service Training Manager
ST	Standby Time

STACCS	Standard Theater Army Command and Control System
STCCS	Strategic and Theater Command and Control Systems
STU	Secure Telephone Unit

## T

T&E	Test and Evaluation
TADT	Total Administrative Delay Time
TAFIM	Technical Architecture for Information Management
TBD	To Be Determined
TCM	Total Corrective Maintenance Downtime
TCP/IP	Transmission Control Protocol/Internet Protocol
TDBM	Technical Database Manager
TDY	Temporary Duty
TEMP	Test and Evaluation Master Plan
TIP	Technology Insertion Project
TIWG	Test Integration Working Group
TLDT	Total Logistics Delay Time
TPM	Total Preventive Maintenance Downtime
TPFDD	Time Phased Force Deployment Data
TRM	Technical Reference Model
TS <sup>3</sup> / TS3	Top Secret Support System

## U-V

UCCS	USCINCEUR Command Center System
UCP	Unified Command Plan
UG	User's Guide
UI	Unit Information
ULSS	User's Logistics Support Summary
UN	United Nations
UM	User's Manual
UPS	Uninterruptable Power Supply
USACOM	United States Atlantic Command
USMC	United States Marine Corps
USTRANSCOM	United States Transportation Command
VPS	Voice Processing System

## **W-X-Y-Z**

WAN	Wide Area Network
WIN	WWMCCS Intercomputer Network
WIS	WWMCCS Information System
WWMCCS	Worldwide Military Command and Control System
WWS	WIS Workstation

**ANNEX B**  
**APPLICABLE GCCS DOCUMENTS**

<u>Document Title</u>	<u>Date</u>	<u>POC</u>	<u>Commercial Phone #</u>	<u>DSN Prefix</u>
1. Mission Need Statement	8 June 95	J6V	(703) 614-5908	224
2. Concept of Operations (CONOPS)	14 Aug 95	J36	(703) 614-0590	224
3. Migration Director Charter	6 Jan 95	D23	(703) 735-8575	653
4. Program Management Plan	29 Mar 95	D23	(703) 735-8507	653
5. Functional Economic Analysis	30 Mar 95	D623	(703) 681-2404	761
6. Test and Evaluation Master Plan	17 Mar 95	JEEXC	(703) 735-8763	653
7. Operational Evaluation Master Plan	11 Jul 95	JEEXC	(703) 735-8763	653
		JITC	(520) 538-5124	879
8. Operational Evaluation Plan	7 Mar 95	JITC	(520) 538-5124	879
		JEEXC	(703)735-8763	653
9. GCCS Training Plan	1 Sep 95	D23	(703) 735-8934	653
10. Joint Integrated Logistics Support Plan	30 Sep 95	D23	(703) 735-8283	653
11. Configuration Management Policy	TBD	J36		
12. Configuration Management Plan	TBD	J36		
13. Migration Strategy	22 Mar 95	D23	(703) 735-8507	653
14. Common Operating Environment	14 Dec 94	JEAC	(703) 735-8758	653
15. Integration Standard	26 Oct 95	JEEXA	(703) 735-8668	653
16. GCCS AIS Security Plan for Ver 2.1	17 Jul 95	JEAC	(703) 735-8784	653
17. JOPEs Training Organization Course Catalog		TRANSCOM	(618) 256-8042	576
18. GCCS Training Plan	March 95	AETC	(601) 377-5377	597
19. Best of the Breed Plan-Draft	January 94	D64	(703) 735-8509	653
20. Software Design Doc. for GCCS COE	11 April 95	D64	(703) 735-8509	653

It should be noted that the majority of the above documents are in Draft formats and are subject to change.



**ANNEX C**  
**DISTRIBUTION LIST**